UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Fernando Carlos Pereira

Criptografia Temporal: Aplicação Prática em Processos de Compra

Dissertação submetida à Universidade Federal de Santa Catarina como parte dos requisitos para a obtenção do grau de mestre em Ciência da Computação.

Prof. Ricardo Felipe Custódio, Dr.
Orientador

Florianópolis, Março de 2003

Criptografia Temporal: Aplicação Prática em Processos de Compra

Fernando Carlos Pereira

Esta Dissertação foi julgada adequada para a obtenção do título de mestre em Ciência da Computação, área de concentração Sistemas de Computação e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciência da Computação.

Prof. Fernando Ostuni Gauthier, Dr.
Coordenador do Curso

Banca Examinadora

Prof. Ricardo Felipe Custódio, Dr.
Orientador

Prof. Carlos Roberto De Rolt, Dr.

Prof. Daniel Santana de Freitas, Dr.

Prof. Joni da Silva Fraga Dr.

Prof. Routo Terada, Dr.

"A sabedoria não nos é dada. É preciso descobri-la por nós mesmos depois de uma viagem que ninguém nos pode poupar ou fazer por nós." (Marcel Proust, escritor francês)

Aos meu pais, Domingos e Iracema.

Agradecimentos

Ao professor Ricardo Felipe Custódio pela dedicação e empenho que orientou a realização deste trabalho, e em especial pelos ensinamentos que me proporcionou.

Aos professores Carlos Roberto de Rolt, Daniel Santana de Freitas, Dalton Francisco de Andrade, Joni da Silva Fraga, Julibio David Ardigo e Routo Terada, pelas importantes contribuições.

Ao meu irmão Fabiano e às minhas irmãs Rosane e Graciela, pela grande amizade que nos une.

À minha namorada Adriana Elissa Notoya pelo carinho, apoio e compreensão, fundamentais na realização deste trabalho.

Aos amigos Anderson Luiz Fernandes Perez, Gilson Anselmo de Araujo, Michel Sehn, Maria Osman e Eliane Pozzebon pela companhia durante os momentos de descontração.

Aos graduandos Iuri Campana e Victor Simas Silva pela ajuda no desenvolvimento do sistema.

E sobretudo a Deus, por conceder-me o dom da vida e a oportunidade de conhecer todas as pessoas a quem agradeço neste momento.

A todos, meu sincero muito obrigado!

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Siglas

AA	Autoridade de Aviso.
AC	Autoridade Certificadora.
AD	Autoridade de Datação.
AR	Autoridade de Registro.
AES	Advanced Encryption Standard.
DES	Data Encryption Standard.
DSA	Digital Signature Algorithm.
DP	Diretório Público.
ECSV	Esquema de compartilhamento de segredos verificável.
ICP	Infra-estrutura de Chaves Públicas.
LabSEC	Laboratório de Segurança em Computação - UFSC.
LCR	Lista de Certificados Revogados.
MIT	Massachusetts Institute of Technology.
NIST	National Institute of Standards and Technology.
PGP	Pretty Good Privacy.
RSA	Rivest-Shamir-Adleman.
SHA-1	Secure Hash Algorithm-1.
SSL	Secure Sockets Layer.
TLS	Transport Layer Security.

Lista de Símbolos

n	Total de participantes do esquema de limiar de Shamir.
t	Limiar do esquema de limiar de Shamir.
h	Índice identificador, onde $h = i, ..., n_C$
i	Índice identificador, onde $i = 1, ..., n_F$
M_i	Membro i de um grupo.
F_i	Fornecedor i.
C_h	Membro h da comissão de licitação.
T	Período de tempo em que o conteúdo de um documento cifrado deve permanecer secreto.
TKr	Chave privada que deve ser mantida secreta durante o período de tempo *T*.
TKu	Chave pública correspondente à *TKr*.
TKr_i	Parte i da chave *TKr*.
M_iTKr	Chave *TKr* pertencente à M_i.
M_iTKr_j	Parte j da chave *TKr* pertencente à M_i.
F_iTKr	Chave *TKr* pertencente à F_i.
F_iTKr_j	Parte j da chave *TKr* pertencente à F_i.
REC( )	Recibo.
R( )	Resumo.
S( )	Assinatura digital.

Resumo

Este trabalho apresenta propostas na linha de pesquisa Segurança e Comércio Eletrônico, constituindo-se de novos protocolos de criptografia temporal e um protocolo criptográfico para envio de propostas em processos de compra.

Os protocolos de criptografia temporal visam assegurar a confidencialidade de documentos eletrônicos durante um determinado período de tempo e garantir que após transcorrido este período, o documento pode ser lido independente da vontade de quem o tornou confidencial.

O protocolo para envio de propostas permite a aplicação prática dos protocolos de criptografia temporal propostos, atendendo a requisitos de segurança que retratam as necessidades inerentes a processos de compra, em particular a processos de licitação pública.

A viabilidade de implementação dos protocolos propostos é demonstrada no desenvolvimento de um sistema, o qual implementa alguns módulos destes protocolos.

Palavras-chave: criptografia, protocolos criptográficos, criptografia temporal, compartilhamento de segredos, licitação pública.

Abstract

This work presents proposals on Security and Electronic Commerce, consisting of applicable timed-release cryptography protocols and a cryptographic protocol for sending of proposals in purchase processes.

The timed-release cryptography protocols aim at assuring the confidentiality of electronic documents during a determined period of time and to guarantee that after this period, the document can be read regardless of the will of those who turned it confidential.

The protocol for sending of proposals allow the application of the timed-release cryptography protocols proposed, taking care of the requirements of security that portray the inherent necessities of purchase processes, in particular the processes of public licitation.

The viability of implementation of the considered protocols is demonstrated in the development of a system which implements some modules of these protocols.

Key words: cryptography, cryptographic protocols, timed-release cryptography, secret sharing, public licitation.

Capítulo 1

Introdução

A capacidade de transmitir dados a longas distâncias em curto tempo e a baixo custo foi um dos fatores que contribuíram para a rápida disseminação do uso da Internet. Hoje, a Internet se mostra como um importante meio de comunicação de alcance mundial onde pessoas, empresas e governos comunicam-se através de simples trocas de mensagens até a realização de transações comerciais e transferência de informações confidenciais. Neste contexto o documento eletrônico se faz cada vez mais presente, servindo como veículo para as informações transmitidas através da Internet.

Tanto na transmissão quanto no armazenamento destes documentos eletrônicos, é necessária a adoção de mecanismos capazes de garantir a sua segurança tornando-os imunes à ação de agentes não autorizados que visam acessá-los ou mesmo destruí-los. Esta necessidade se deve ao fato que muitas vezes estes documentos são sigilosos por conterem informações particulares como números de cartões de crédito, dados pessoais e informações bancárias.

A segurança pode ser obtida com a utilização de recursos da Tecnologia de Segurança da Informação que possui suas bases fixadas sobre a criptografia e seus serviços.

A Internet, aliada a estes recursos de segurança, criou um ambiente capaz de suportar diversas aplicações de negócio, antes somente disponíveis no mundo real[1],

[1]Mundo real: termo utilizado para referenciar o mundo físico em que vivemos e onde utiliza-se documentos em meio papel.

como aplicações bancárias, livrarias e supermercados. As qualidades oferecidas por este novo ambiente são muitas, tais como: alcance mundial, agilidade, dinamismo, segurança, comodidade, conveniência, economicidade e lucratividade.

Tanto no mundo real quanto no chamado mundo eletrônico, existem aplicações que exigem confidencialidade às suas informações e o controle sobre o tempo em que estas são mantidas confidenciais. Estas aplicações possuem como requisito a garantia de que uma determinada informação permanecerá confidencial durante um determinado período de tempo, e após transcorrido este período deve ser assegurado o acesso a informação mesmo que alguém seja contra.

No mundo real, uma das formas utilizadas para suprir esta necessidade é a utilização de envelopes selados por lacres de segurança, abertos somente após a ocorrência de um determinado evento. Antes da abertura do envelope é verificada a integridade do lacre a fim de constatar se houve ou não violação. Podemos citar algumas destas aplicações para melhor contextuação:

- *Licitações Públicas*: exige que as propostas comerciais dos licitantes[2] sejam entregues em envelopes lacrados que somente podem ser abertos em data e hora pré-determinadas;
- *Testamentos*: devem ter seu conteúdo revelado somente após a morte do testador;
- *Provas a serem aplicadas com finalidade de avaliação*: devem ser mantidas em sigilo a fim de evitar que terceiros tomem conhecimento das questões antes do devido momento;
- *Informações governamentais secretas*: devem ser mantidas em sigilo por um determinado período de tempo.

Este trabalho busca propor soluções, com o apoio da Tecnologia de Segurança da Informação, que proporcionem o controle sobre o período de tempo em que informações devem ser mantidas secretas, às aplicações que necessitam deste requisito. Em particular, este trabalho visa propor soluções que permitam que o envio de

[2]Licitantes: Participantes do processo de licitação que pretendem contratar com a administração pública.

propostas comerciais em processos de licitação pública, enquadrados em determinadas modalidades, seja realizado através da Internet.

1.1 Definição do Problema

Muitas empresas, principalmente o governo brasileiro, adotam para os seus processos de compra um modelo baseado no recebimento de propostas comerciais em envelopes selados por lacres de segurança e que somente são abertos a partir da ocorrência de um evento futuro previamente estabelecido. Este evento refere-se a uma sessão pública ocorrida em dia e hora pré-estabelecidos, onde são abertos os envelopes que contém as propostas. A violação do conteúdo de um destes envelopes acarreta a destruição total ou parcial do lacre de segurança e conseqüentes danos ao envelope, deixando evidente o ato praticado. Em casos onde ocorre a violação de uma proposta, as partes envolvidas podem facilmente verificar o ocorrido e então tomar as providências previstas em lei.

A implementação deste modelo de envio de propostas via Internet encontra como principal dificuldade o controle confiável sobre o tempo em que as propostas devem permanecer confidenciais, e ainda, assegurar que no momento devido elas poderão ser abertas mesmo sem o auxílio do fornecedor que a compôs.

Em uma primeira análise, algumas soluções podem parecer triviais, tais como:

- **Solução 1:** o fornecedor utiliza uma chave secreta para cifrar sua proposta que é posteriormente enviada ao comprador. Na data em que ocorre o evento de abertura de propostas, o fornecedor procede com o envio da chave secreta ao comprador a fim de possibilitar que este decifre a sua proposta;

- **Solução 2:** o fornecedor deixa a chave secreta necessária à decifragem da sua proposta sob a guarda de uma terceira entidade confiável, a qual responsabiliza-se por entregar a chave ao comprador somente na data de abertura de propostas;

- **Solução 3:** uma terceira entidade confiável gera um par de chaves assimétricas e divulga a chave pública deste par para que os fornecedores a utilizem na cifragem de suas propostas. A chave privada do par é mantida em sigilo até a data do evento de abertura de propostas.

Em cenários ideais, onde todos os envolvidos no processo são confiáveis, estas soluções podem realmente ser utilizadas para a resolução do problema. Porém devemos considerar que vivemos em uma sociedade onde nem todas as pessoas são confiáveis, principalmente quando se trata de defender seus interesses particulares. Portanto é necessário criar soluções onde seja garantida a inviolabilidade das propostas até o momento da abertura, sem que para isso seja necessário confiar nos participantes do processo de licitação.

Situações onde inexiste confiança entre os participantes, ou mesmo situações onde os participantes não se mostram confiáveis, invalidam automaticamente as soluções apresentadas acima. A tabela 1.1 relaciona estas situações.

Tabela 1.1: Situações que invalidam soluções que dependem da existência de confiança mútua entre os participantes de um processo de licitação.

Solução	Situação que invalida a solução
1	O fornecedor, por algum motivo, se nega a enviar sua chave secreta.
2	Os participantes do processo se negam a confiar em uma terceira entidade ou sua confiabilidade é colocada em dúvida.
3	Idem à segunda situação.

Estas situações tornam evidente que a tarefa de manter um documento eletrônico confidencial por algum tempo, e a partir da ocorrência de determinado evento futuro garantir o acesso ao seu conteúdo, independente da vontade de quem o tornou confidencial, não é trivial.

Em síntese, o que se busca alcançar são soluções no mundo do documento eletrônico que proporcionem as mesmas condições de segurança e conforto proporcionado no mundo papel pelo uso do lacre de segurança no envelope que contém a proposta.

1.1.1 Requisitos de Segurança

A construção de protocolos criptográficos ou mesmo de sistemas eletrônicos que visam prover segurança a processos de compras, em particular processos de licitação pública, deve considerar vários requisitos de segurança, os quais retratam as necessidades e regulamentações inerentes a estes processos. Esta seção descreve estes requisitos. Alguns foram descritos em trabalhos científicos, dos quais vale citar o de Michiharu Kudo [KUD 98], os demais requisitos foram estabelecidos com base nas exigências que constam na legislação brasileira que regulamenta estes processos.

Os requisitos de segurança estabelecidos são descritos abaixo:

1. **Anonimato:** Ninguém pode conhecer a identidade dos fornecedores antes da abertura das propostas ou divulgação do resultado;

2. **Verificabilidade:** O fornecedor deve receber provas de que sua proposta foi entregue dentro do prazo devido;

3. **Temporalidade:** Nenhuma proposta pode ser entregue fora do período de entrega das propostas;

4. **Unicidade:** Cada fornecedor tem o direito de concorrer com uma única proposta;

5. **Confidencialidade:** O conteúdo das propostas deve ser secreto e inviolável até o momento previsto para a sua abertura;

6. **Integridade:** O conteúdo de uma proposta submetida ao processo deve ser inalterável;

7. **Autonomia:** Na fase de abertura das propostas, qualquer proposta deve poder ser aberta sem a necessidade de interação com o fornecedor que a compôs;

8. **Irrefutabilidade (não-repúdio):** Uma vez entregue a proposta e aberta, no momento devido, ela se torna irrevogável e irrefutável por parte do fornecedor que a compôs;

9. **Não Coerção:** O fornecedor não pode provar ou identificar uma oferta, antes da data de abertura de propostas;

10. **Legalidade (licitude):** Não deve ser possível um participante praticar atos ilícitos no processo de compra;

11. **Disponibilidade:** Após a abertura da proposta, qualquer pessoa, participante ou não do processo, deve poder ter acesso ao conteúdo desta, inclusive da vencedora;

12. **Auditoria Interna:** Todos os participantes do processo devem poder verificar a correta implementação do mesmo;

13. **Auditoria Externa:** Todo o processo de compra deve poder ser verificável por terceiros previamente estabelecidos.

A Lei 8.666/93, a qual regulamenta os processos de compra das administrações públicas no Brasil, estabelece os princípios jurídicos sobre os quais devem ser conduzidos os processos de compra, a fim de conferir-lhes a legalidade e transparência necessárias. A tabela 1.2 demonstra o enquadramento de cada um dos requisitos de segurança estabelecidos em relação a estes princípios.

Tabela 1.2: Enquadramento dos requisitos de segurança em relação aos princípios jurídicos.

Princípios	**Requisitos de segurança que atende**
Isonomia	1, 2, 3, 4, 7 e 9
Legalidade	2, 3, 4, 5, 6, 8, 10, 11, 12 e 13
Moralidade	10
Igualdade	1, 3, 4, 5, 6 e 12
Impessoalidade	6 e 8
Publicidade	11, 12 e 13
Economicidade	-
Probidade Administrativa	10
Vinculação ao Instrumento Convocatório	3, 4 e 8
Julgamento Objetivo	-

Os princípios jurídicos são conceituados na seção 5.3.2, página 64.

1.2 Objetivos

1.2.1 Objetivo Geral

Propor protocolos criptográficos que possibilitem a decifragem de um documento eletrônico somente após transcorrido um determinado período de tempo ou em um evento futuro previamente especificado, independente da vontade de quem o cifrou.

1.2.2 Objetivos Específicos

- Analisar a legislação brasileira que ampara os processos de compra de entidades públicas;
- Estabelecer requisitos de segurança necessários a processos de compra realizados através de licitação pública;
- Propor um protocolo criptográfico para envio, via Internet, de propostas comerciais em processos de licitação pública, cujas modalidades são voltadas para compras e indisponíveis em meio eletrônico, que vise atender aos requisitos de segurança estabelecidos;
- Aplicar na prática os protocolos criptográficos criados para atender ao objetivo geral;
- Analisar os protocolos propostos quanto ao atendimento aos requisitos de segurança estabelecidos;
- Desenvolver um sistema via Internet que implemente alguns módulos dos protocolos propostos, a fim de demonstrar a viabilidade de implementação.

Neste trabalho são considerados somente os processos de compra realizados por empresas públicas, sendo considerados somente aqueles que se baseiam no modelo de recebimento e análise de propostas comerciais entregues em envelopes lacrados e mantidos desta forma até o evento oficial de abertura de propostas.

1.3 Materiais e Métodos

O desenvolvimento deste trabalho está apoiado, essencialmente, em pesquisas bibliográficas sobre técnicas e protocolos criptográficos e sobre processos de compra de entidades públicas.

Utilizou-se para estas pesquisas artigos científicos, dissertações de mestrado, teses de doutorado, leis e livros que abordam assuntos como: processos de compra, criptografia e segurança da informação.

As pesquisas sobre processos de compras de entidades públicas se realizou por meio das atuais leis brasileiras que regulamentam o assunto, e por meio de entrevistas com ex-integrantes[3] da comissão permanente de licitação da Universidade Federal de Santa Catarina (CPL/UFSC).

No desenvolvimento do sistema, foram utilizadas as seguintes tecnologias:

- Linguagens de programação PHP [PHP 02], VBScript [MIC 02e], JavaScript [MIC 02c] e HTML [W3C 02];
- Servidor Web Apache [APA 02];
- Banco de dados MySQL [MYS 02];
- Ferramenta OpenSSL [OPE 02];
- Biblioteca de suporte a criptografia Capicom [MIC 02a];
- Navegador Internet Explorer [MIC 02d].

[3]Os entrevistados foram o professor Antônio Noronha, membro e presidente da CPL/UFSC de 1985 à 1997, e o sr. Gelvane Francisco Goedert, atual Procurador Federal na UFSC e ocupante por vários anos do cargo de presidente da CPL/UFSC.

1.4 Trabalhos Correlatos

Dentre os materiais pesquisados não foram encontradas propostas, voltadas para processos de compras, que atendessem aos requisitos de segurança estabelecidos. Em alguns trabalhos relativos à venda pública (Leilão) [KUD 98, HAR 98, STU 99, SUZ 02, LIP 02] são apresentados protocolos criptográficos que visam a garantia de apenas alguns destes requisitos de segurança.

Relacionados à garantia de que um documento eletrônico não poderá ser lido durante um determinado período de tempo, estão os trabalhos pioneiros de Timothy C. May [MAY 93] e de Ronald L. Rivest, Adi Shamir e David A. Wagner [RIV 96], nos quais foram traçadas as diretrizes que norteiam a criptografia temporal.

Ainda relativo à criptografia temporal, podem ser destacados os trabalhos de Wenbo Mao [MAO 00, MAO 01] e de Dan Boneh e Moni Naor [BON 00], onde foram propostos protocolos que possibilitam a verificação estrutural de um dos métodos utilizados em esquemas de criptografia temporal, o quebra-cabeça. Não menos importantes, os trabalhos de Michiharu Kudo e Anish Mathuria [KUD 99] e de Giovanni Di Crescenzo e Rafail Ostrovsky e Sivaramakrishnan Rajagopalan [CRE 99] contribuíram com propostas de esquemas de criptografia temporal baseados em entidades confiáveis.

1.5 Justificativa e Motivação

A migração para a Internet de aplicações e serviços dos mais diversos segmentos de negócio existentes no mundo é uma tendência. Dentre estes serviços e aplicações estão os processos de compra realizados pelas empresas.

Assim como pessoas beneficiam-se da comodidade e conveniência proporcionadas pelo comércio eletrônico, as empresas também estão buscando estes benefícios a fim de aumentar suas oportunidades de negócios e diminuir os gastos operacionais tidos com a execução e controle dos seus processos de compra.

Como exemplo, pode ser citada a empresa brasileira Usiminas[4] que ado-

[4] www.usiminas.com.br

tou uma solução via Internet para os seus processos de compra e alcançou uma redução média de 80% no custo com comunicação, 50% no tempo de levantamento de cotações de preços, diminuição de 35% no tempo gasto durante todo o processo, economia de 80% nos gastos com papel e uma redução de 95% no tempo gasto com digitação [MIC 02b]. Podem ser citadas ainda empresas estatais como a Caixa Econômica Federal e o Banco do Brasil ou mesmo o próprio governo federal com o seu portal de compras, o **Comprasnet**[5].

Em essência, este trabalho visa proporcionar soluções para aplicações que exigem o controle sobre o tempo de confidencialidade de suas informações. No campo das compras eletrônicas, também chamado de *e-procurement*, este trabalho visa propor meios para tornar possível a implementação segura via Internet do procedimento de envio de propostas comerciais, utilizado em processos de compra estruturados sobre o modelo de licitação pública onde utiliza-se o envio de envelopes lacrados ao comprador. Estes procedimentos são ainda indisponíveis através da Internet por carência de soluções que atendam às suas necessidades.

Este trabalho está inserido no projeto **Cartório Virtual** do Laboratório de Segurança em Computação (LabSEC) - UFSC. O Cartório Virtual tem por objetivo propiciar, via Internet, todos os serviços de um cartório tradicional. Desta maneira os cidadãos poderão ter acesso a estes serviços na comodidade de sua casa ou escritório, utilizando-se da tecnologia Segura da Informação. No contexto deste projeto, este trabalho contribui para viabilizar a implementação via Internet de serviços oferecidos por cartórios, que exijam que uma informação seja mantida secreta durante um determinado período de tempo e que possa ser acessada somente a partir da ocorrência de um evento no futuro, tal como a abertura de um testamento após a morte de uma pessoa.

1.6 Organização do Texto

Este trabalho está estruturalmente organizado em capítulos. O capítulo 2 apresenta conceitos de criptografia que serão fundamentais para o entendimento de assuntos descritos nos capítulos posteriores. No capítulo 3 são descritos em detalhes o

[5] www.comprasnet.gov.br

funcionamento, os tipos e os aspectos de segurança dos esquemas de compartilhamento de segredos utilizados nas soluções apresentadas por este trabalho. O capítulo 4 conceitua criptografia temporal, cita as aplicações onde ela é requerida e descreve o funcionamento dos esquemas existentes. O capítulo 5 apresenta conceitos relativos a processos de compra e enfatiza a sua abordagem em entidades públicas. O capítulo 6 apresenta novos protocolos criptográficos que visam fornecer serviços de criptografia temporal a grupos. Estes protocolos, juntamente com o protocolo descrito no capítulo subseqüente, fazem parte das propostas deste trabalho. O capítulo 7 apresenta um protocolo criptográfico destinado a garantir a segurança de propostas comerciais, enviadas por meio eletrônico, em processos de licitação pública, nas modalidades concorrência, tomada de preços e convite. Por fim as considerações finais sobre o trabalho desenvolvido são apresentadas no capítulo 8.

Capítulo 2

Fundamentos de Criptografia

2.1 Introdução

A criptografia hoje é o alicerce principal de muitas aplicações do mundo eletrônico. A segurança e integridade de informações das mais variadas espécies dependem fundamentalmente dos serviços fornecidos pela criptografia.

Este trabalho utiliza-se de diversos conceitos da criptografia para alcançar seus objetivos, por este motivo torna-se essencial a compreensão destes conceitos.

A seção 2.2 apresenta conceitos de criptografia e de algoritmos simétricos e assimétricos. A seção 2.3 apresenta o conceito de função resumo, uma ferramenta de extrema importância principalmente para as assinaturas digitais, conceituadas na seção 2.4. A seção 2.5 descreve o funcionamento da infra-estrutura de chaves públicas. Na seção 2.6 é apresentada uma Rede de Misturadores, ferramenta utilizada para prover anonimato às entidades envolvidas em comunicações eletrônicas. Na seção 2.7 é apresentado o conceito de protocolo de documentos eletrônicos, ferramenta de grande importância para situar no tempo, de maneira segura, documentos e eventos eletrônicos. A seção 2.8 apresenta o conceito de módulo criptográfico de hardware, o qual é utilizado para prover segurança em sistemas que armazenam e manipulam informações sensíveis. Por fim, a seção 2.9 apresenta o conceito da autoridade de aviso, entidade que garante o não repúdio na entrega de documentos eletrônicos ao seu destinatário.

2.2 Criptografia

Criptografia é a ciência de comunicar-se de forma secreta através da escrita em códigos. A palavra criptografia deriva da junção das palavras gregas *kriptos* (secreto, oculto) e *grifo* (grafia). No passado essa técnica foi largamente utilizada em guerras e conflitos para a comunicação secreta entre exércitos aliados. Hoje, é o principal meio utilizado para proteger informações digitais de pessoas, empresas e governos.

Proteger o conteúdo de um documento eletrônico por meio da criptografia consiste em codificar este documento através do processo denominado *cifragem* de modo que somente indivíduos autorizados são capazes de decodificar este documento, através do processo inverso denominado *decifragem*, tornando-o novamente inteligível. Um documento eletrônico em sua forma original é denominado *texto original* e quando codificado, *texto cifrado*.

Os processos de cifragem e decifragem de dados são realizados através de algoritmos criptográficos específicos. Estes algoritmos utilizam chaves criptográficas em conjunto com os textos originais ou cifrados (dependendo do processo a ser realizado).

Chaves criptográficas são números utilizados para programar o algoritmo criptográfico e são enquadradas em dois tipos: *chaves simétricas*, utilizadas em algoritmos criptográficos simétricos (este conceito será apresentado na seção 2.2.1) e *chaves assimétricas*, utilizadas em algoritmos criptográficos assimétricos (este conceito será apresentado na seção 2.2.2). A importância das chaves criptográficas é definida pelo princípio de Kerckhoff [SCH 96], o qual diz que a segurança de um algoritmo criptográfico deve residir inteiramente nas chaves criptográficas utilizadas e não no ocultamento do seu mecanismo de funcionamento.

Os principais serviços da criptografia utilizados para prover segurança às informações, são [MEN 96, STA 98]:

Confidencialidade: garante que as informações protegidas serão acessíveis somente a entidades autorizadas;

Integridade: assegura que uma informação não sofreu modificações ou destruição, se-

jam elas acidentais ou cometidas por agentes maliciosos[1];

Autenticação: identifica de maneira segura uma entidade;

Irrefutabilidade (não-repúdio): garante que uma entidade não possa negar uma ação praticada por ela.

Ao sistema que reúne um conjunto de objetos utilizados para prover um ou mais destes serviços, dá-se o nome de criptossistema. Segundo a teoria de Shannon [STI 95] a segurança de um criptossistema é classificada como:

Computacionalmente seguro: quando o melhor ataque conhecido para quebrar o sistema requer um poder computacional maior do que o existente no momento ou em futuro próximo ou ainda que leve um tempo superior ao da vida útil das informações asseguradas por ele;

Incondicionalmente seguro: retrata o criptossistema ideal, aquele onde mesmo utilizando o melhor ataque criptoanalítico e infinitos recursos computacionais disponíveis não é suficiente para quebrar o sistema.

Atacar um criptossistema significa tentar obter o texto original a partir do cifrado sem o conhecimento da chave criptográfica. As formas de atacar um criptossistema são: $i)$ através da *força bruta*, que consiste em testar todas as possíveis chaves até encontrar a correta; $ii)$ através de *técnicas de criptoanálise*, que buscam recuperar o texto original em um tempo menor do que o gasto pelo ataque de força bruta, utilizando para isso técnicas específicas. Quando o ataque é bem sucedido, dizemos que o criptossistema foi *quebrado*.

Os algoritmos criptográficos dividem-se em dois grupos que são diferenciados pela forma como utilizam as chaves criptográficas. São eles: *algoritmos de chave simétrica* e *algoritmos de chave assimétrica*.

[1]Agente Malicioso: indivíduo mal intencionado que busca beneficiar-se de maneira ilícita das informações de suas vítimas.

2.2.1 Algoritmos de Chave Simétrica

Estes algoritmos são caracterizados por utilizarem a mesma chave criptográfica no processo de cifragem e decifragem das informações. Esta chave deve ser secreta e de conhecimento único e exclusivo dos indivíduos envolvidos diretamente na comunicação.

A utilização da criptografia simétrica em uma comunicação segura, deve ser precedida do compartilhamento da chave secreta entre os comunicantes. Este compartilhamento deve ser feito através de um canal de comunicação seguro, como por exemplo a entrega pessoal da chave criptográfica.

Os principais algoritmos simétricos utilizados atualmente são: DES [NIS 93a, STA 98, STI 95] e AES [NIS 01a].

2.2.2 Algoritmos de Chave Assimétrica

O conceito de algoritmos assimétricos, também chamados de algoritmos de chaves públicas, foi introduzido em 1976 por Whitfield Diffie e Martin Hellman [DIF 76].

Ao contrário dos algoritmos simétricos, os assimétricos utilizam um par de chaves criptográficas no processo de cifragem e decifragem das informações: a *chave pública* que é amplamente divulgada e acessível a todos, e a sua correspondente, a *chave privada*, que deve ser secreta e de uso único e exclusivo do seu proprietário.

Para o estabelecimento de uma linha de comunicação segura utilizando algoritmos assimétricos, não existe a necessidade da comunicação ser precedida do compartilhamento de chaves como exigido em algoritmos simétricos, basta que o remetente utilize a chave pública do destinatário, acessível através de um local público, para cifrar a mensagem. A mensagem cifrada com uma determinada chave pública só pode ser decifrada pela correspondente chave privada. Isto garante que apenas o real destinatário da mensagem terá acesso ao seu conteúdo, uma vez que ele deve utilizar a sua chave privada no processo de decifragem. Na prática todavia, os algoritmos assimétricos são usados para trocar chaves de sessão, que por sua vez são chaves de um algoritmo simétrico.

Os algoritmos assimétricos possuem dentre suas aplicações, a garantia de autenticidade através de assinaturas digitais e a garantia da confidencialidade através da cifragem de informações.

O algoritmo assimétrico mais conhecido e utilizado atualmente é o RSA [RIV 78]. Alguns outros exemplos são [MEN 96]: ElGamal, McEliece e Knapsack.

2.3 Função Resumo

Função resumo é uma função que aplicada sobre um documento eletrônico, independente do seu tamanho, gera um resumo de tamanho fixo [SCH 96]. O resumo de uma mensagem também possui outras denominações tais como *hash*, *message digest* e *fingerprint*.

Estas funções são utilizadas para garantir a integridade dos dados no processo de assinatura digital [STI 95, SCH 96]. O resumo representa a impressão digital de um documento, identificando-o de forma única, daí a sua empregabilidade nos serviços de garantia de integridade de dados e assinaturas digitais. Um documento que sofre alterações, por menores que sejam, dificilmente produz o mesmo resumo que o documento original. Esta característica é utilizada na verificação de eventuais alterações não-autorizadas sofridas pelo documento.

Ao ser projetada, uma função resumo h deve atender a determinadas propriedades [MEN 96]:

1. **Compressão:** aplicando a função h sobre um bloco de dados x de qualquer tamanho, resultará em uma saída y de tamanho fixo;

2. **Fácil computação:** tendo a função h e a entrada x, é relativamente fácil computar $h(x)$;

3. **Caminho único:** é impraticável computacionalmente deduzir o valor de entrada x a partir do valor de saída y;

4. **Fraca resistência a colisão:** dado x, é impraticável encontrar um valor x' tal que $h(x) = h(x')$;

5. **Forte resistência a colisão:** é impraticável computacionalmente encontrar duas entradas distintas, x e x', que produzam o mesmo resumo.

O algoritmo padrão para geração de resumos definido pelo Instituto Nacional de Padrões e Tecnologia Americano (NIST) é o SHA-1 (Secure Hash Algorithm-1) [NIS 93b].

Alguns outros algoritmos utilizados na geração de resumos são [MEN 96]: MD4, MD5 e RIPEMD-160.

2.4 Assinatura Digital

Análoga a assinatura manuscrita em documento papel, a assinatura digital é utilizada para identificar de maneira única o autor da assinatura. Suas aplicações no campo de segurança de dados são muitas, principalmente nos serviços de autenticação, integridade de dados e não-repúdio [MEN 96].

A geração de assinaturas digitais depende de um *algoritmo de geração de assinatura digital* e a validação destas assinaturas é feita através do *algoritmo de verificação de assinatura digital*. Ambos os algoritmos são baseados nos fundamentos da criptografia assimétrica.

Para produzir uma assinatura digital sobre um documento eletrônico, este é submetido ao algoritmo de geração de assinatura junto com a chave privada do signatário. Na validação desta assinatura o algoritmo de verificação de assinatura utiliza a chave pública do suposto signatário para avaliar a autenticidade da assinatura, a qual somente é considerada autêntica caso tenha sido produzida utilizando a chave privada respectiva a esta chave pública.

A autenticidade de uma assinatura digital é garantida pela forma como ela é gerada, ou seja, o emprego da chave privada no algoritmo de geração de assinatura

presume o consentimento do proprietário da chave, uma vez que ela deve ser de conhecimento e uso único e exclusivo seu. O não-repúdio também se utiliza deste conceito, já que um suposto signatário não pode negar ter assinado um documento eletrônico se a assinatura neste puder ser validada através da sua chave pública.

Por meio da comparação dos resumos calculados na origem e no destino, pode ser verificada a integridade de um documento. Na prática assinaturas digitais não são feitas diretamente sobre os documentos, mas sim sobre os seus resumos [HOU 01]. Este procedimento aumenta a eficiência dos algoritmos de assinatura e verificação, pois isenta a necessidade de trabalhar com documentos muito grandes.

Assinaturas digitais podem ser aliadas à datação eletrônica de documentos (apresentado na seção 2.7) para comprovar que um documento foi assinado em um tempo específico [STI 95]. Isto é útil, por exemplo, em casos onde é necessário comprovar que assinaturas feitas em um dado período não são válidas. Um destes casos é o comprometimento da chave privada de uma pessoa, tornando possível que elementos maliciosos que tenham tido acesso àquela chave privada assinem documentos em seu nome.

O algoritmo padrão americano para geração e verificação de assinaturas digitais definido pelo Instituto Nacional de Padrões e Tecnologia Americano (NIST) é o DSA (Digital Signature Algorithm) [NIS 00] que utiliza o algoritmo SHA-1 para geração de resumos.

Além do DSA, o algoritmo RSA em conjunto com o algoritmo SHA-1 é muito utilizado na geração de assinaturas digitais [STA 98] .

Alguns outros algoritmos utilizados são [MEN 96]: ElGamal, Schnorr, Fiat-Shamir, ESIGN.

2.5 Infra-estrutura de Chaves Públicas

Infra-estrutura de Chaves Públicas (ICP) consiste em um conjunto de componentes e serviços necessários à utilização da criptografia de chaves-públicas. Estes componentes e serviços são responsáveis por criar, gerenciar, armazenar e distribuir certificados digitais de chave pública.

Certificado digital ou certificado de chave pública é um documento eletrônico que associa de forma segura o valor de uma chave pública a uma pessoa ou entidade. Sua emissão é feita por uma Autoridade Certificadora, a qual assina o certificado a fim de conferir veracidade aos seus dados. O formato mais conhecido para certificados digitais é definido pela recomendação ITU-T X.509 [FOR 97, HOU 01]. Os campos que basicamente o compõem são: formato do certificado, número serial, identificador do algoritmo de assinatura digital utilizado pelo emissor para assinar o certificado, dados do emissor, dados do sujeito (pessoa ou entidade para a qual o certificado está sendo emitido), a chave pública do sujeito e período de validade do certificado.

Os componentes básicos presentes em uma ICP e responsáveis por criar, gerenciar, armazenar e distribuir certificados digitais são: *Autoridade Certificadora (AC)*, *Autoridade de Registro (AR)* e *Diretório Público (DP)*. Suas conceituações seguem nas seções subseqüentes.

A certificação digital é de fundamental importância para o comércio eletrônico e também para outras transações realizadas via internet que necessitem garantir a autenticidade e confidencialidade de suas informações. Aplicações que utilizam-se de assinaturas digitais e cifragem de dados são algumas das aplicações beneficiadas pelos certificados digitais.

A figura 2.1 apresenta de forma geral o funcionamento e a interação entre componentes de uma Infra-estrutura de Chaves Públicas.

2.5.1 Autoridade Certificadora

A Autoridade Certificadora (AC) é a entidade responsável pela emissão de certificados digitais e pelo controle dos certificados revogados e expirados.

A emissão de um certificado digital tem início quando a AC recebe uma requisição contendo os dados identificadores do solicitante e sua chave pública. Após a comprovação dos dados, feita de acordo com políticas e padrões pré-estabelecidos, o certificado digital é assinado pela AC. Uma cópia do certificado é então enviada ao solicitante e outra ao diretório público.

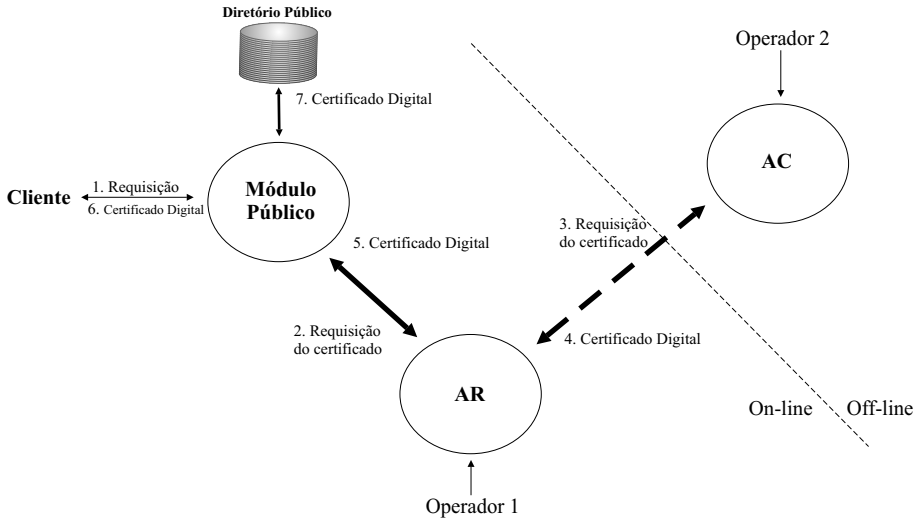

Figura 2.1: Infra-estrutura de chaves públicas: O cliente envia uma requisição ao módulo público. Estes dados são remetidos à Autoridade de Registro para validação. Após a validação, a AR submete a requisição à AC, a qual emite e publica o certificado digital.

Após a emissão e o recebimento do certificado, o até então solicitante passa a ser denominado assinante dos serviços disponibilizados pela Infraestrutura de Chaves Públicas.

A revogação de um certificado digital é de responsabilidade exclusiva da AC e pode ser motivada por um situação específica, por exemplo, por uma solicitação do assinante sob a alegação de que sua chave privada foi comprometida.

Os certificados revogados por uma Autoridade Certificadora são inseridos em uma *Lista de Certificados Revogados (LCR)* emitida e assinada pela própria AC. As LCR são disponibilizadas publicamente, possibilitando que usuários de certificados digitais verifiquem se um certificado digital está ou não revogado, seja para gerar a assinatura como para conferir. As LCR devem ser atualizadas em um período de tempo adequado a fim de evitar que certificados revogados sejam considerados válidos por motivo de desatualização da LCR.

2.5.2 Autoridade de Registro

A Autoridade de Registro (AR) é uma entidade na qual a Autoridade Certificadora confia e delega a tarefa de averiguação e comprovação dos dados submetidos pelos solicitantes para emissão dos certificados digitais.

A averiguação e comprovação dos dados obedece a políticas e padrões pré-definidos. Algumas das maneiras utilizadas para a validação dos dados fornecidos pelo solicitante são: a verificação de documentos, a solicitação da presença física do solicitante e comprovação de que o solicitante possui a chave privada correspondente à chave pública submetida para a emissão do certificado [FOR 97].

Em determinadas situações, a Autoridade Certificadora pode delegar a função de averiguação e comprovação dos dados do solicitante a mais de uma AR. Útil para situações onde ocorre a existência de muitos usuários potenciais em regiões geograficamente distantes. A estas AR dá-se o nome de *Autoridade de Registro Local (ARL)* [FOR 97].

2.5.3 Diretório Público

Diretório Público (DP) é a entidade responsável pela publicação dos certificados digitais e das LCR.

É através dos Diretórios Públicos que usuários podem obter os certificados digitais que eles pretendem utilizar. O DP não dispõe de mecanismos que garantam a autenticidade e integridade dos dados que ele armazena. Estes requisitos são obtidos através da verificação da assinatura digital feita pela AC sobre os certificados e as LCR.

Os Diretórios Públicos são, em sua maioria, estruturados com base na recomendação ITU-T X.500 e em sua versão simplificada LDAP [HOU 01].

2.6 Rede de Misturadores

O conceito de rede de misturadores foi introduzido por David L. Chaum [CHA 81]. Em seu trabalho, Chaum apresentou uma solução para prover anonimato às

pessoas envolvidas em comunicações eletrônicas, utilizando uma entidade denominada *misturador*, cujo propósito é ocultar a correlação entre as mensagens que recebe e as mensagens que transmite.

Misturadores são utilizados como entidades intermediárias entre grupos comunicantes, mantendo anônimos os integrantes do grupo que envia mensagens ao outro grupo. Em seu funcionamento mais básico, um misturador recebe como entrada um conjunto de mensagens eletrônicas de tamanho único. Caso alguma mensagem não possua o tamanho definido, é anexado uma cadeia de bits aleatórios a fim de lhe conferir o tamanho necessário. O procedimento de expansão da mensagem é necessário para impossibilitar a associação de mensagens de entrada com mensagens de saída através dos seus tamanhos. As mensagens são enviadas ao misturador pelos seus respectivos remetentes, que possuem as responsabilidades de complementá-las com a cadeia de bits quando necessário e cifrá-las com a chave pública do misturador.

Internamente o misturador decifra as mensagens utilizando a sua chave privada, descarta as cadeias de bits aleatórios nos casos em que se fizeram necessárias e permuta as mensagens do conjunto a fim de eliminar a correlação de ordenação entre as mensagens de entrada e saída. Por fim, o misturador encaminha as mensagens aos seus devidos destinatários. Os destinatários das mensagens não são capazes de identificar os remetentes iniciais, pois o misturador elimina os dados identificadores destes e então assume o papel de remetente das mensagens.

Em casos onde há a possibilidade de falha do misturador, utiliza-se um conjunto de misturadores para a execução da tarefa, eliminando assim o efeito destas possíveis falhas. Este conjunto de misturadores recebe a denominação de *rede de misturadores*, também chamada de *cascata de misturadores*.

Em uma rede de misturadores, cada misturador desempenha as mesmas tarefas executadas em aplicações com apenas um misturador. O misturador recebe os dados cifrados com sua chave pública, decifra-os com sua chave privada e envia-os ao seu destinatário, que neste caso é o próximo misturador da rede. Ao último misturador da rede cabe a tarefa de encaminhar as mensagens aos seus reais destinatários.

Segundo Jakobsson *et al* [JAK 02], uma rede de misturadores conside-

rada robusta deve:

Operar corretamente: corresponder a uma permutação entre o conjunto de mensagens de saída e as mensagens do conjunto de entrada;

Prover Privacidade: eliminar a correlação de identificação e ordenação entre as mensagens de entrada e saída;

Ser Robusta: fornecer uma prova ou fortes evidências de que a operação de permutação foi realizada corretamente, e permitir que qualquer uma das partes envolvidas seja capaz de verificar a veracidade do processo através desta prova ou evidências.

Uma das formas para se auditar o funcionamento de uma rede de misturadores é solicitar de forma aleatória que seja revelada parcialmente a relação entre mensagens de entrada e mensagens de saída de cada misturador, mas de forma a não permitir que seja traçado o caminho de qualquer mensagem do início até o fim da rede.

Redes de misturadores são de grande importância em aplicações onde é imprescindível o anonimato do seu usuário, tais como votação digital [JAK 02] e pagamento eletrônico [JAK 98].

2.7 Protocolo de Documentos Eletrônicos

O protocolo de documentos eletrônicos serve ao mesmo propósito que o protocolo feito em documentos papel, que é adicionar dados de data ao documento.

A localização temporal confiável de documentos eletrônicos é requisito essencial na utilização destes documentos em transações eletrônicas ou em caráter legal. Há muitos exemplos da utilização da data de um documento na resolução de disputas entre partes, tais como: na comprovação de que um determinado documento foi assinado após o comprometimento da chave privada do suposto signatário; na comprovação de que o testamento foi assinado antes ou depois do falecimento do testador; na comprovação de que uma proposta comercial foi entregue dentro do prazo definido em um edital de

licitação; na resolução de disputas por patentes onde ganha quem possui o registro de patente mais antigo.

Serviços de protocolo de documentos são conjuntos de técnicas e métodos responsáveis por autenticar temporalmente documentos. Podem ser estruturados através da *confiança distribuída* entre os usuários do serviço ou através de uma *Autoridade de Datação (AD)*, sendo este último o modelo mais utilizado.

Serviços baseados em confiança distribuída são utilizados entre grupos de datadores. Neste modelo, vários integrantes do grupo datam e assinam digitalmente o documento, ao término deste processo o documento é considerado datado. Este modelo possui desvantagens em relação à sua eficiência pois o documento deve ser protocolado por todos os datadores.

Já os serviços baseados em uma AD partem do pressuposto de que esta é uma entidade confiável e que toda uma comunidade de usuários do serviço compartilham desta confiança. Neste modelo, o documento é enviado pelo cliente à AD, esta anexa ao documento um selo de tempo (autenticação temporal) e assina digitalmente o conjunto $documento/selo\ de\ tempo$. A AD envia um recibo contendo o selo de tempo e a assinatura ao cliente e mantém uma cópia deste documento datado em sua base de dados com o propósito de resolver disputas futuras. Este processo de datação é ilustrado na figura 2.2.

O funcionamento de uma Autoridade de Datação pode ser periodicamente auditado através da verificação dos registros de log de suas operações.

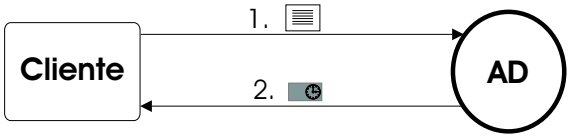

Figura 2.2: Mecanismo de datação de documentos eletrônicos: 1. Cliente envia um documento eletrônico à AD. 2. AD envia um recibo contendo o selo de tempo assinado.

Serviços de protocolo de documentos devem atender aos seguintes requisitos de segurança [PAS 02]:

Privacidade: O conteúdo do documento deve ser de conhecimento exclusivo do cliente;

Canal de comunicação e armazenamento: O tamanho do documento não deve afetar no desempenho do serviço de protocolo;

Disponibilidade: Deve ser assegurado o funcionamento permanente do serviço de protocolo e também a integridade dos dados;

Anonimato: O cliente deve ter sua identidade mantida em sigilo;

Confiança: Garante que um documento não será protocolado com data diferente da atual.

2.7.1 Uso de Funções Resumo na Datação Eletrônica

Na prática os documentos eletrônicos não são datados, mas sim seus resumos. Por possuir a propriedade de representar de maneira única um documento eletrônico, a utilização do resumo atende o propósito do serviço e ainda traz consigo ganhos relativos a:

Privacidade: Impede que terceiros tomem conhecimento do conteúdo do documento;

Desempenho: A transmissão e o protocolo do resumo é mais eficiente quando comparada à transmissão e protocolo do documento, pois o resumo é normalmente muito menor do que o documento que o originou;

Armazenamento: O espaço necessário para armazenar os resumos é menor do que o espaço que seria necessário para armazenar documentos de diversos tamanhos.

2.7.2 Autenticação Temporal Absoluta x Relativa

Existem dois tipos de autenticação temporal, a absoluta e a relativa [ROO 99]. A autenticação absoluta confere ao documento eletrônico uma localização exata no tempo, utilizando-se de valores tais como data, hora, minuto, segundo.

Na autenticação relativa, o tempo é representado por valores que possibilitam apenas determinar se um documento foi datado antes ou depois de outro documento.

Em modelos que utilizam autenticação absoluta, é necessário que a referência temporal seja obtida de uma fonte única e confiável.

Já em modelos que utilizam-se da autenticação relativa, a datação de documentos é feita através de esquemas de encadeamento entre os documentos, que consiste em ligar o documento corrente a um ou mais de seus antecessores através de funções de caminho único [BUL 98, ROO 99].

2.7.3 Implementações Comerciais de Autoridades de Datação Eletrônicas

O LabSEC/UFSC possui o projeto *Protocoladora Digital de Documentos Eletrônicos (PDDE)* no qual existem diversos pesquisadores trabalhando no desenvolvimento e aprimoramento de novas tecnologias de protocolo de documentos eletrônicos. O LabSEC conta com o apoio da empresa **Bry Tecnologia**[2], para a qual são repassadas as tecnologias desenvolvidas.

No cenário mundial, as implementações comerciais de maior destaque são as soluções oferecidas pelas empresas **Datum**[3] e **TimeProof**[4].

2.8 Módulos Criptográficos de Hardware

Módulos criptográficos de hardware são mecanismos que executam serviços específicos de criptografia, como por exemplo cifragem de dados, autenticação, assinatura digital e gerenciamento de chaves criptográficas [NIS 01b]. Estes módulos podem ser constituídos por hardware, software e firmware[5], ou pela combinação destes elementos.

A criação e utilização destes dispositivos exige a adoção de políticas de segurança eficazes que estabeleçam regras e procedimentos a serem seguidos desde o

[2] www.bry.com.br

[3] www.datum.com

[4] www.timeproof.de

[5] Firmware: programas que são armazenados de forma permanente em chips de hardware.

projeto até o gerenciamento do dispositivo. Estas políticas devem ser definidas com base nos requisitos de segurança do sistema onde o módulo atuará, no ambiente onde ele será utilizado e nos serviços de segurança que serão oferecidos.

O Instituto Nacional de Padrões e Tecnologia americano (NIST) estabelece através do padrão FIPS PUB 140-2 [NIS 01b] requisitos de segurança necessários ao projeto e implementação de módulos criptográficos nos Estados Unidos. Neste padrão são especificados quatro níveis de segurança:

Nível 1: garante um baixo nível de segurança. Nele são enquadrados módulos onde a implementação de controles de segurança física e lógica é limitada ou mesmo inexistente, não havendo o controle dos softwares que operam sobre o módulo.

Nível 2: garante um nível de segurança mais elevado que o nível anterior. Os módulos aqui enquadrados se diferenciam pela adoção de controles de segurança física. Para obter acesso ao conteúdo de um módulo enquadrado neste nível é necessário transpor barreiras físicas de proteção.

Além dos controles físicos de acesso, também são adotados controles lógicos de autenticação baseado em papéis, nos quais determinado tipo de usuário terá acesso apenas aos serviços que foram atribuídos privilégio de acesso ao papel que ele possui.

Neste nível são feitas exigências quanto aos softwares que operam sobre o módulo.

Nível 3: Os controles de segurança física deste nível são mais rígidos que os do nível anterior, e visam proteger as informações internas do módulo. O módulo pode ser mantido em um ambiente totalmente protegido por barreiras físicas e pode possuir sensores para detecção de tentativas de acessos físicos. Uma tentativa de violação ao módulo pode ocasionar, inclusive, uma reação de auto defesa que resulte na destruição de todas as informações críticas de segurança mantidas pelo módulo.

A entrada ou saída no módulo, de informações críticas de segurança ocorre através de portas de comunicação separadas fisicamente das demais. Outro requisito para este nível é que todas as informações de segurança que entram ou saem do módulo,

somente podem ser feitas em sua forma cifrada ou quebradas por esquemas de compartilhamento de segredos.

O controle de acesso é baseado em identificação, onde somente certos indivíduos ganharão acesso aos serviços do módulo.

Neste nível são feitas exigências quanto aos softwares que operam sobre o sistema.

Nível 4: O mais alto nível de segurança estabelecido. A segurança física protege por completo o módulo de toda e qualquer tentativa de acesso. Na ocorrência de acessos físicos não autorizados, os mecanismos de auto-defesa são imediatamente acionados e destroem todas as informações críticas de segurança mantidas pelo módulo.

A proteção física também engloba o cuidado com as variáveis de temperatura e voltagem presentes no ambiente onde é mantido o módulo e os cuidados para que qualquer flutuação nestas variáveis não afetem a sua segurança.

Assim como no nível 3, a comunicação de informações críticas de segurança com o mundo exterior ocorre por portas fisicamente separadas das demais e as informações que entram ou saem do módulo, devem estar cifradas ou quebradas por esquemas de compartilhamento de segredos.

O controle de acesso também é baseado em identificação.

Neste nível são feitas exigências quanto aos softwares que operam sobre o sistema.

Um maior detalhamento de todas as especificações de segurança de módulos criptográficos estabelecidas através do padrão FIPS PUB 140-2 é encontrado em [NIS 01b].

2.9 Autoridade de Aviso

A *Autoridade de Aviso (AA)* é uma entidade confiável que possui a função de estabelecer a comunicação entre duas partes quando uma destas recusa-se ou encontra-se incapaz de receber e confirmar o recebimento de um documento eletrônico [CUS 01].

A Autoridade de Aviso pode utilizar diversos meios para atingir o seu objetivo, tais como: publicações em diretórios públicos, em periódicos eletrônicos ou em meio papel, fóruns e serviços de entrega manual, como os correios. Todos os passos executados pela AA são registrados em um relatório e publicados em diretório público.

O serviço fornecido pela Autoridade de Aviso possui similaridade a serviços utilizados no mundo real, tais como cartas registradas ou intimações judiciais entregues por oficiais de justiça.

As figuras 2.3 e 2.4 ilustram o funcionamento de uma Autoridade de Aviso.

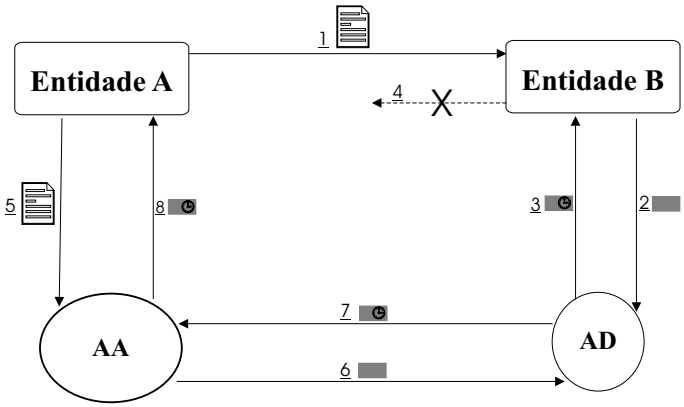

Figura 2.3: Funcionamento da Autoridade de Aviso: 1^a Fase - 1. Entidade A envia um documento à Entidade B. 2. A Entidade B pode, eventualmente, protocolar o documento recebido. 3. Neste caso a AD envia o recibo de protocolo. 4. Por algum motivo a Entidade A não recebe, da Entidade B, a confirmação de recebimento. 5. A Entidade A envia então o documento à AA para que esta tome as providências cabíveis para realizar a entrega do documento à Entidade B. 6. AA protocola o recebimento do documento. 7. A AD envia o recibo à AA. 8. A AA envia à Entidade A a confirmação do recebimento do documento.

2.10 Conclusão

Neste capítulo foram apresentados conceitos que serão utilizados para entendimento do restante deste trabalho. Estes conceitos aliados aos conceitos de Compartilhamento de Segredos e Criptografia Temporal, explicados nos dois capítulos seguintes, formarão a base das soluções apresentadas por este trabalho.

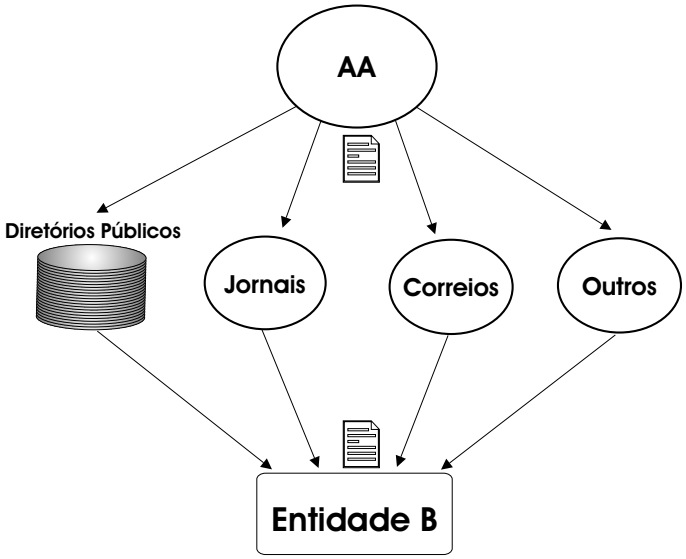

Figura 2.4: 2^a Fase - Nesta fase a AA utiliza-se de diversos meios (publicações em diretórios públicos, em periódicos eletrônicos ou em meio papel e serviços de entrega manual, como os correios) para realizar a entrega do documento à Entidade B.

Capítulo 3

Compartilhamento de Segredos

3.1 Introdução

Protocolos, ou esquemas de compartilhamento de segredos são importantes ferramentas utilizadas em situações onde não há confiança entre um grupo de entidades ou em situações onde há risco de destruição e perda da informação (segredo). Estes esquemas dividem um segredo entre um grupo de entidades e obrigam que parte delas estejam presentes no momento em que for necessário fazer uso do segredo. O segredo a ser compartilhado pode ter as mais variadas naturezas, sendo a mais usual o compartilhamento de chaves criptográficas.

Alguns exemplos que podemos citar são:

Situação 1: Através de longo trabalho conjunto, um grupo de químicos descobriu um novo e revolucionário medicamento. A fórmula deste medicamento precisa então ser guardada em um lugar seguro até ser patenteada, porém os químicos não possuem confiança mútua entre si. Então, quem guardaria a fórmula? A solução seria utilizar um esquema de compartilhamento de segredos para compartilhar a fórmula entre os químicos. Quando desejarem patentear o novo medicamento, basta que um determinado número deles una suas parcelas para obter a fórmula;

Situação 2: A criação de *backup* de uma informação não é recomendável pois a coloca sob o risco de roubo devido a facilidade existente em se copiar dados eletrônicos.

> A solução é utilizar um esquema de compartilhamento de segredos para dividir a informação em partes e então guardá-las em diferentes locais. Quando necessário, basta unir algumas destas partes e então reconstruir a informação.

A idéia por trás do compartilhamento de segredos consiste na aplicação do conceito de *confiança distribuída*, o qual visa a descentralização do controle de informações, tornando desnecessário que uma informação seja deixada sob o controle de uma única entidade. Desta maneira o controle é distribuído para um grupo de entidades que a princípio devem ser confiáveis. Entretanto, mesmo se algumas se mostrarem hostis ou conspirarem entre si, a informação permanecerá segura, desde que o número mínimo de entidades necessárias à reconstrução da informação não seja alcançado pelo grupo hostil.

Neste capítulo são descritos em detalhes o funcionamento, os tipos e os aspectos de segurança de esquemas de compartilhamento de segredos. Estes esquemas serão utilizados em alguns dos protocolos propostos no capítulo 6, com o objetivo de utilizar, nestes protocolos, o conceito de *confiança distribuída* e com isso tornar todos os membros de um grupo responsáveis pela manutenção da confidencialidade dos documentos eletrônicos cujo conteúdo se pretende ocultar durante um determinado período de tempo.

A seção 3.2 introduz os conceitos básicos de compartilhamento de segredos. Na seção 3.3 é apresentado um esquema de compartilhamento básico que utiliza a operação matemática *ou exclusivo*, ou simplesmente *xor*, para dividir o segredo. Na seção 3.4 é descrito em detalhes o funcionamento de esquemas baseados em limiares. Na seção 3.5 é abordado o conceito de compartilhamento verificável e também o funcionamento de esquemas que possibilitam a verificação da veracidade das partes distribuídas aos participantes. A seção 3.6 trata dos esquemas de compartilhamento de segredos onde o segredo é construído de maneira cooperativa pelos próprios participantes, tornando desnecessária a existência de uma terceira entidade responsável por dividir e distribuir o segredo entre os participantes. Por fim, a seção 3.7 descreve o serviço de compartilhamento de segredos oferecido pelo programa PGP - Pretty Good Privacy.

3.2 Conceitos e Funcionamento

Esquemas de compartilhamento de segredos são esquemas que permitem dividir um segredo em pedaços, chamados de partes, os quais são entregues aos participantes de um grupo tal que somente subconjuntos autorizados destes participantes são capazes de reconstruir o segredo unindo suas partes, mas subconjuntos não autorizados são incapazes de obter qualquer informação sobre o segredo.

Subconjunto autorizado é aquele que possui o número mínimo de participantes necessários para a reconstrução do segredo, já um conjunto não autorizado é aquele que possui um número de participantes menor do que o necessário para a reconstrução do segredo.

Um esquema de compartilhamento de segredos consiste em uma entidade confiável, doravante denominada juiz, um conjunto, denotado $\mathcal{P}$, de n participantes $P_1, ..., P_n$ e uma estrutura de acesso a qual define os subconjuntos de participantes capazes de reconstruir o segredo.

Para compartilhar um segredo s o juiz quebra este segredo em n partes s_i, onde $i = 1, ..., n$, e as distribui entre um conjunto de n participantes P_i, $i = 1, ..., n$, que posteriormente poderão reconstruir o segredo através da junção de algumas destas partes.

Existem diversas aplicações práticas para estes esquemas na área de segurança de dados, principalmente no que diz respeito à proteção da confidencialidade e integridade de chaves criptográficas. Uma delas é o controle de operações críticas onde duas ou mais pessoas são necessárias para realizar a operação. Outra é a divisão de responsabilidades entre um grupo de pessoas, de forma que uma determinada ação se realiza apenas se um certo número de pessoas cooperarem entre si.

A distribuição das partes aos participantes do esquema, merece atenção especial, pois durante a comunicação entre juiz e participante um agente malicioso pode obter informação suficiente para comprometer todo o esquema. Uma forma de distribuir as partes de maneira segura é utilizar canais de comunicação privados entre juiz e participantes. Outra maneira é utilizar criptografia assimétrica cifrando as partes dos segredos

com as chaves públicas dos respectivos destinatários.

Serão considerados na descrição dos esquemas de compartilhamento de segredos três protocolos: de construção, de distribuição e o de reconstrução.

Protocolo de construção: define os parâmetros iniciais do esquema, tais como o segredo, o número de participantes e a estrutura de acesso. A partir destes parâmetros, o juiz configura o esquema e então gera as partes do segredo;

Protocolo de distribuição: envolve a distribuição das partes do segredo obtidas no protocolo de construção. Estas partes são distribuídas pelo juiz, de maneira segura, aos participantes;

Protocolo de reconstrução: compreende a reconstrução do segredo feita através da união das partes de um subconjunto autorizado de participantes.

3.2.1 Estrutura de Acesso

A estrutura de acesso representa o conjunto, denotado $\mathcal{A}$, de todos os subconjuntos autorizados a reconstruir um determinado segredo.

Um subconjunto autorizado é aquele que reúne participantes em um número igual ao mínimo exigido para a reconstrução de um segredo.

Exemplo: Considere que um segredo foi compartilhado entre 3 participantes (P_1, P_2, P_3) e o número mínimo de participantes exigidos para a sua reconstrução é 2, então teremos a seguinte estrutura de acesso.

$$\mathcal{A} = \{(P_1, P_2), (P_1, P_3), (P_2, P_3)\}$$

Em esquemas de compartilhamento de segredos, a estrutura de acesso é representada como (t, n). Utilizando o exemplo citado acima, a estrutura de acesso é representada como (2, 3).

Em termos matemáticos, a estrutura de acesso representa a combinação de n elementos, t a t.

Segundo Douglas R. Stinson [STI 95], um esquema de compartilhamento de segredos realizado sob uma estrutura de acesso $\mathcal{A}$ é considerado perfeito, se as seguintes propriedades forem satisfeitas:

1. se um subconjunto autorizado de participantes $A \subseteq \mathcal{P}$ unir suas partes, eles poderão determinar o valor de s;

2. se um subconjunto não autorizado de participantes $A \subseteq \mathcal{P}$ unir suas partes, eles não poderão determinar informação alguma sobre o valor de s.

Sendo o conjunto $\alpha \in \mathcal{A}$ e $\alpha \subseteq \beta \subseteq \mathcal{P}$, o conjunto β é considerado um superconjunto de α, o que lhe atribui a capacidade de também determinar o valor do segredo s. Quando se tem esta situação, a estrutura de acesso satisfaz a propriedade *monotone* [STI 95], ou seja:

$$\alpha \in \mathcal{A} \text{ e } \alpha \subseteq \beta \subseteq \mathcal{P}, \text{ então } \beta \in \mathcal{A}.$$

3.3 Divisão do Segredo

O esquema de *divisão do segredo* [SCH 96] divide um segredo s entre duas ou mais pessoas, seguindo o seguinte protocolo:

1. Toma-se conhecimento do valor de n (número de participantes);

2. Um juiz gera $n-1$ números aleatórios do mesmo tamanho de s. Os números são identificados por x_i sendo $i = 1, ..., n-1$;

3. O juiz calcula: $s \oplus x_1 \oplus x_2 \oplus ... \oplus x_{n-1} = y$, onde $\oplus$ representa a operação *ou-exclusivo (xor)*;

4. O juiz entrega x_i para P_i, sendo $i = 1, ..., n-1$, e y para P_n:

Para reconstruir o segredo os participantes unem suas partes e realizam a operação inversa:

$$s = y \oplus x_1 \oplus x_2 \oplus ... \oplus x_{n-1}$$

Este esquema é considerado muito seguro, já que uma pessoa isolada não obtém informação alguma sobre o segredo caso não una sua parte com as partes de todos os outros participantes. Em essência, é utilizada uma função **one-time-pad**[1] para cifrar o segredo, e as chaves são distribuídas entre os participantes.

Este esquema também pode ser implementado utilizando outras operações matemáticas, tais como soma ou subtração. O protocolo de compartilhamento permanece o mesmo descrito acima, substituindo-se somente a operação *xor* pela operação desejada.

Entretanto, este esquema possui a desvantagem de que todos os participantes devem contribuir com as suas partes para tornar possível a reconstrução do segredo. Portanto, se algum deles se negar a entregar ou mesmo ter sua parte do segredo destruída por algum motivo, o segredo não poderá mais ser recuperado.

A figura 3.1 apresenta um exemplo deste esquema.

3.4 Esquemas de Limiar (t, n)

Criados independentemente por George R. Blakley e Adi Shamir [SHA 79], os esquemas de Limiar são métodos pelos quais uma entidade confiável calcula n partes s_i, $i = 1, ..., n$, de um segredo s, e as distribui secretamente entre os participantes P_i, $i = 1, ..., n$, tal que um subconjunto de t participantes, $t \leq n$, pode reconstruir o segredo s unindo as suas partes. Entretanto, se um subconjunto menor que t participantes tentar reconstruir o segredo, não obterá informação alguma sobre ele.

São dois os parâmetros utilizados neste esquema. O primeiro parâmetro t é chamado de limiar do esquema, o qual define o número de participantes que cooperando entre si, podem reconstruir o segredo inicialmente dividido. O segundo parâmetro

[1] Funções one-time-pad garantem uma segurança incondicional ao esquema e ainda possuem a vantagem de ser de fácil utilização [STI 95].

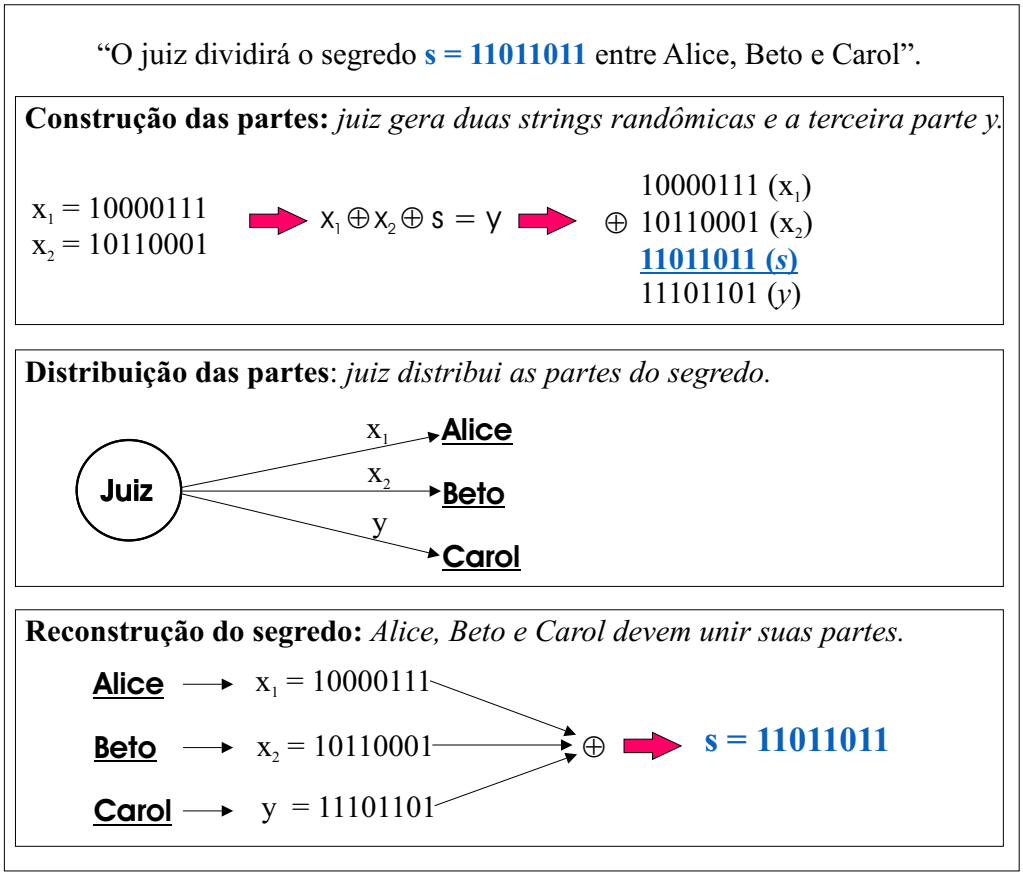

Figura 3.1: Exemplo do Protocolo de Divisão do Segredo utilizando a operação matemática *xor*.

n representa o número total de participantes do esquema, entre os quais ocorre a divisão do segredo.

Shamir definiu em seu trabalho propriedades necessárias a um esquema de limiar [SHA 79, MEN 96]:

Perfeito: o esquema é considerado perfeito quando conhecendo-se $t-1$ ou menos partes do segredo, não é possível determinar o segredo correto;

Ideal: quando o tamanho das partes é igual ao tamanho do segredo;

Extensível para novos usuários: deve ser possível calcular novas partes do segredo para serem entregues a novos participantes, sem que para isso as partes já distribuídas sejam afetadas;

Controle Hierárquico: pode ser delegado maior poder a determinado usuário, simplesmente entregando-lhe mais partes do segredo.

3.4.1 Esquema do Limiar de Shamir

Baseado na interpolação de polinômios onde as partes do segredo são representadas por pontos em um plano bi-dimensional (x_i, y_i), $i = 1, ..., n$. O valor de x_i é determinado pelo juiz para cada um dos participantes e então tornado público. O valor de y_i é secreto e entregue a cada participante individualmente. A segurança deste esquema está no fato de haver um e somente um polinômio $f(x)$ de grau $t - 1$ tal que $f(x_i) = y_i$ para todo i [SHA 79].

Neste trabalho a coordenada x_i será representada pelos mesmos valores da variável i e a coordenada y_i será representada pelos valores das partes s_i do segredo.

Os parâmetros iniciais do esquema são: *o segredo, o número de participantes* e *o valor do limiar*. Definidos estes parâmetros o juiz configura a estrutura do esquema, iniciando com a seleção de um número primo p maior que o segredo e que o número de participantes. No passo seguinte, o juiz cria um polinômio de grau $t - 1$ cujos coeficientes são valores aleatórios pertencentes ao conjunto Z_p e no qual o coeficiente a_0 é a representação numérica do segredo a ser dividido.

$$f(x) = s + \sum_{j=1}^{t-1} a_j x^j (mod\ p)$$

A geração das partes é feita submetendo ao polinômio os valores de x_i. Cada valor s_i gerado deve ser entregue ao seu respectivo participante P_i.

$$s_i = f(x_i) = s + \sum_{j=1}^{t-1} a_j (x_i)^j (mod\ p)$$

A reconstrução do segredo é feita através da união das partes s_i de um subconjunto autorizado de t participantes. Estes participantes deverão revelar suas partes s_i e então utilizarem-se de interpolação polinomial para determinar os coeficientes do polinômio $f(x)$. Determinando estes coeficientes, conseqüentemente o segredo s será encontrado, já que este é representado pelo coeficiente a_0.

Os coeficientes do polinômio $f(x)$ podem ser determinados pela *fórmula de interpolação de Lagrange* [MEN 96] [STI 95]:

$$f(x) = \sum_{j=1}^{t} b_j s_{(i_j)} \quad \text{onde} \quad b_j = \prod_{1 \leq k \leq t,\ k \neq j} \frac{x - x_{(i_k)}}{x_{(i_j)} - x_{(i_k)}}$$

Uma simplificação pode ser feita se o objetivo é somente encontrar o coeficiente $a_0 = s$. Considerando $f(0) = a_0 = s$, a equação é expressa da seguinte forma [MEN 96, STI 95]:

$$s = \sum_{j=1}^{t} b_j s_{(i_j)} \quad \text{onde} \quad b_j = \prod_{1 \leq k \leq t,\ k \neq j} \frac{x_{(i_k)}}{x_{(i_k)} - x_{(i_j)}}$$

Embora existam muitas técnicas de interpolação polinomial, a fórmula de Lagrange é a mais usada em esquemas de compartilhamento de segredos. Todas as outras fórmulas forneceriam uma expressão muito mais complicada para s.

Como exemplo, construiremos um esquema de limiar onde o juiz divide o segredo $s = 11$ respeitando a estrutura de acesso (3, 5) a qual define que o segredo será compartilhado entre 5 participantes respeitando um limiar igual a 3. Abaixo segue a descrição do exemplo através dos protocolos de construção, distribuição e reconstrução.

Protocolo de construção: São informados ao juiz os parâmetros iniciais: $s = 11$, $n = 5$ e $t = 3$.

O juiz escolhe o número primo $p = 31$ e constrói um polinômio de grau $t - 1$ cujos coeficientes são determinados aleatoriamente, exceto o coeficiente a_0 que representará o segredo $s = 11$. A figura 3.2 ilustra a geração das partes do segredo a partir do polinômio criado.

Protocolo de distribuição: Cada uma das partes geradas é entregue aos participantes através de um canal de comunicação seguro. A figura 3.3 ilustra a distribuição das partes do segredo aos participantes.

Protocolo de reconstrução: Supomos que os participantes que desejam cooperar a fim de reconstruir o segredo sejam P_1, P_3 e P_5. Cada revela a sua parte do segredo e então utilizam a fórmula de Interpolação de Lagrange para obter o valor do segredo s. A figura 3.4 ilustra a reconstrução do segredo a partir das partes s_1, s_3 e s_5.

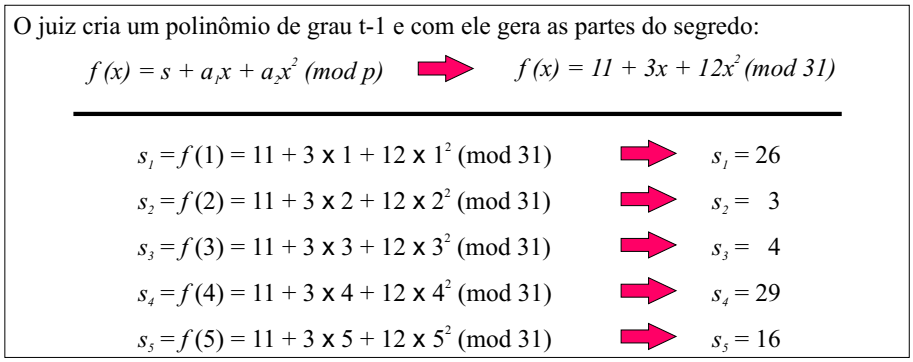

Figura 3.2: Esquema do Limiar de Shamir - Protocolo de construção: O juiz cria as partes s_i do segredo através do polinômio $f(x)$.

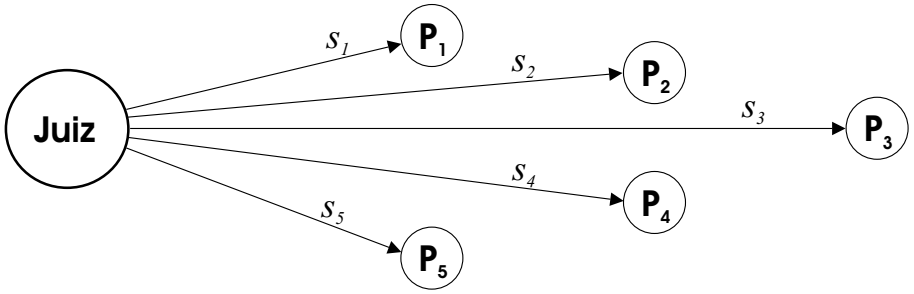

Figura 3.3: Esquema do Limiar de Shamir - Protocolo de distribuição: O juiz distribui aos participantes as partes s_i criadas no protocolo de construção.

Também é possível implementar o esquema de divisão do segredo utilizando o esquema do Limiar de Shamir. Basta que o valor do limiar (t) seja igual ao número total de participantes (n), desta maneira temos uma estrutura de acesso (n, n).

3.5 Compartilhamento de Segredos Verificável

Esquema de compartilhamento de segredos verificável (ECSV) [STA 96, GEN 96, SCH 99, STI 99] é utilizado para garantir a segurança de um esquema de compartilhamento contra a ação de participantes maliciosos, que possam cometer atos prejudiciais tais como [SCH 99]:

- Um juiz malicioso distribui partes falsas do segredo aos participantes;

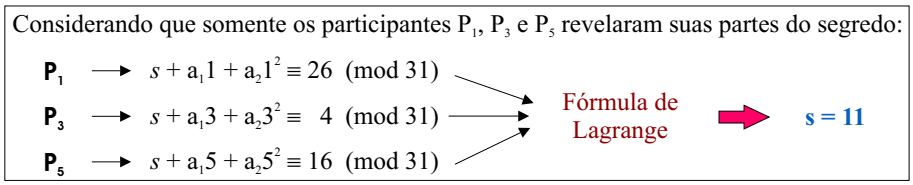

Figura 3.4: Esquema do Limiar de Shamir - Protocolo de reconstrução: A reconstrução do segredo é realizada através de interpolação polinomial utilizando um número mínimo de partes do segredo distribuídas entre os participantes.

- Participantes maliciosos enviam partes falsas do segredo durante o protocolo de reconstrução.

ECSV permite que participantes do esquema verifiquem a integridade das partes que recebem e com isso tenham certeza de que conseguirão recuperar o segredo em questão. Também torna possível excluir participantes desonestos ou mesmo aqueles, que por algum outro motivo, reproduziram suas partes do segredo com imperfeições.

3.5.1 Esquema de Compartilhamento de Segredos Verificável

Esta seção apresenta um esquema que possibilita a verificabilidade das partes de um segredo. A verificabilidade das partes consiste em determinar se uma parte do segredo é ou não o logaritmo discreto de um elemento publicamente conhecido. Este esquema foi descrito por Markus Stadler [STA 96].

A compreensão de alguns conceitos é necessária para possibilitar o entendimento deste esquema, são eles:

Logaritmo Discreto: é o valor do expoente α, proveniente da operação $y = x^{\alpha}(mod\ p)$. Em termos matemáticos, o valor de α é descrito como $log_x y(mod\ p)$;

Problema do Logaritmo Discreto: este problema é considerado de elevada complexidade dada a dificuldade existente em determinar o valor de α conhecendo-se apenas os valores de x, y e p, sendo p um número primo muito grande;

Conjuntos Z_p e Z_p^*: Z_p representa o conjunto de números inteiros de ordem[2] p. Z_p^* é o grupo multiplicativo de ordem $\phi(p)$, sendo $\phi(p) = p - 1$;

Elemento Gerador: um elemento g pertencente ao conjunto Z_p^*, sendo p um número primo, é chamado *elemento gerador* ou *elemento primitivo* se e somente se for possível escrever qualquer elemento $\varepsilon \in Z_p^*$ como $\varepsilon = g^i \ (mod\ p)$, sendo $0 \leq i \leq p - 2$.

No protocolo de construção deste esquema, utiliza-se o esquema de Shamir (seção 3.4.1) para dividir o segredo. A verificabilidade das partes é feita através do protocolo de verificação por cada um dos participantes, no momento em que eles recebem a parte do segredo que lhes cabe. As variáveis iniciais necessárias são:

- A estrutura de acesso (t, n);
- O segredo s;
- Um número primo p, maior que s e que n;
- Um número gerador g do conjunto Z_p^*;

Protocolo de construção: O juiz escolhe aleatoriamente coeficientes $a_j \in Z_p$, sendo $j = 1, ..., t - 1$. Em seguida o juiz calcula $S = g^s \ (mod\ p)$ e $A_j = g^{a_j} \ (mod\ p)$ para cada um dos valores de j.

Os valores g, S e A_j's são publicados pelo juiz em uma área onde todos os participantes do esquema têm acesso. Desta maneira o juiz compromete-se com todos a dividir o segredo s utilizando um polinômio criado pelos coeficientes a_j.

No passo seguinte o juiz usa o esquema do Limiar de Shamir para dividir o segredo, usando um polinômio constituído do segredo s e dos coeficientes a_j escolhidos anteriormente.

Protocolo de verificação: Cada parte s_i é enviada ao participante P_i, sendo $i = 1, ..., n$.

[2]Ordem de um conjunto: representa o número de elementos que o conjunto possui.

Após receber a sua parte do segredo, o participante pode iniciar a verificação da integridade da parte recebida. Esta verificação é realizada através da seguinte equação:

$$S_i = S \prod_{j=1}^{t-1} A_j^{(x_i)^j} (mod\ p)$$

A parte recebida somente será considerada correta se $S_i = g^{s_i}\ (mod\ p)$. Caso seja considerada incorreta, ou seja, $S_i \neq g^{s_i}\ (mod\ p)$, o participante deve relatar o ocorrido a todos os demais e então abortar o processo de compartilhamento.

Podemos provar que a equação $S_i = g^{s_i}\ (mod\ p)$ garante a correção de s_i com base nas seguintes afirmações:

- Sendo $s_i = s + a_1 x_i + ... + a_{t-1}(x_i)^{t-1}\ (mod\, p)$, então $g^{s_i} = g^{s\ +\ a_1 x_i\ +\ ...\ +\ a_{t-1}(x_i)^{t-1}}$ $(mod\, p)$;
- Assumindo que $S_i = S\ .\ A_1^{(x_i)^1}\ .\ ...\ .\ A_{t-1}^{(x_1)^{t-1}}\ (mod\, p)$ e $g^{s\ +\ a_1 x_i\ +\ ...\ +\ a_{t-1}(x_i)^{t-1}} = S\ .\ A_1^{(x_i)^1}\ .\ ...\ .\ A_{t-1}^{(x_1)^{t-1}}\ (mod\ p)$. Temos, portanto, $g^{s_i} = S_i\ (mod\ p)$.

O protocolo de verificação também deve ser executado no momento em que os participantes se reunirem para reconstruir o segredo. Desta maneira é possível constatar se um ou mais participantes divulgaram partes incorretas, prejudicando assim a reconstrução do segredo.

3.6 Compartilhamento de Segredos Sem o Auxílio de uma Entidade Confiável

Em todos os esquemas vistos até agora, uma terceira entidade confiável (o juiz) era responsável por dividir o segredo entre os participantes do esquema, desta forma o juiz sempre conhecia o valor do segredo, entretanto, em muitas situações é desejável que ninguém conheça o segredo antes do momento devido.

Esquemas de *compartilhamento de segredos sem o auxílio de uma entidade confiável* [ING 91, PED 91, JAC 95, STI 99] são caracterizados pela inexistência da

figura do juiz. Nestes esquemas o segredo é construído cooperativamente pelos integrantes do grupo, sendo que cada um deles contribui com uma parte secreta para a construção de um segredo que somente será conhecido quando um conjunto mínimo de participantes unir suas parcelas.

Ingemar Ingemarsson e *Gustavus J. Simmons* [ING 91], apresentaram em seu trabalho um esquema onde cada integrante de um determinado grupo escolhe aleatoriamente um valor para ser a sua contribuição. O segredo é o resultado da união das contribuições enviadas pelos participantes do esquema. Esta união pode ser obtida utilizando alguma operação matemática, por exemplo a soma.

Para que a reconstrução do segredo se torne possível, deve haver a cooperação de todos os indivíduos que contribuíram para a construção do segredo, a menos que estes compartilhem suas partes do segredo utilizando o esquema do Limiar de Shamir conforme será visto na seção 3.6.1.

Uma aplicação prática para o protocolo de Ingemarsson e Simmons está na criação de códigos de acesso. Por exemplo: a abertura do cofre de uma empresa pode ser condicionada à presença dos cinco diretores da empresa. Para tornar isto possível, cada um dos diretores escolhe um código e o insere no mecanismo do cofre, que por sua vez construirá um código único a partir da união dos códigos inseridos. Quando for necessário abrir o cofre, todos os diretores deverão inserir, no mecanismo do cofre, novamente as suas parcelas do código para que ele possa ser reconstruído e o cofre aberto.

3.6.1 Criação Compartilhada de Chaves Assimétricas

Torben Pryds Pedersen [PED 91], propôs um esquema onde os participantes constroem cooperativamente um par de chaves assimétricas. A chave pública do par é construída nas etapas iniciais do esquema e então disponibilizada para o uso dos integrantes do grupo, já a chave privada permanece desconhecida, mesmo porque ela ainda não foi construída. A chave privada somente será conhecida no momento em que um subconjunto autorizado de participantes se empenhar em construí-la.

O esquema de Pedersen baseia-se no *criptossistema de chave pública*

ElGamal, o qual tem sua segurança baseada no problema do logaritmo discreto [STI 95, MEN 96]. Seu funcionamento consiste em escolher um número primo p grande, um elemento gerador g pertencente a Z_p^* e um número aleatório α, tal que $1 \leq \alpha \leq p-2$. A chave privada do esquema é representada por α e a chave pública por β, onde $\beta = g^{\alpha}\ (mod\ p)$. Para cifrar uma mensagem x utilizando o criptossistema ElGamal, deve-se escolher um número inteiro aleatório $k \in Z_{p-1}$ e então calcular:

$$y_1 = g^k\ mod\ p \quad \text{e} \quad y_2 = x.\beta^k\ mod\ p$$

A mensagem cifrada é representada por y_1 e y_2, $c_x = (y_1, y_2)$. Para decifrar x, deve-se calcular:

$$x = d_x(y_1, y_2) = y_2(y_1^{\alpha})^{-1}\ mod\ p.$$

Os passos que compõem o esquema de Pedersen são:

1. Os n participantes escolhem, em comum acordo, um número primo p grande e um elemento gerador $g \in Z_p^*$;

2. O participante P_i, $i = 1, ..., n$, escolhe um número $x_i \in Z_p$ de maneira aleatória e calcula $h_i = g^{x_i}\ (mod\ p)$. Em seguida P_i envia h_i aos demais participantes;

3. Após todos os n participantes terem executado este procedimento, a chave pública h pode ser calculada individualmente através da equação:

$$h = \prod_{i=1}^{n} h_i\ (mod\ p)$$

4. Neste momento, todos os participantes conhecem a chave pública h, entretanto não são capazes de determinar sozinhos a chave privada x que é calculada através da equação:

$$x = \sum_{i=1}^{n} x_i\ (mod\ p)$$

Para ser possível calcular a chave privada, todos os participantes devem contribuir com os seus valores de x_i (escolhidos no passo 2).

O passo seguinte consiste em possibilitar que quaisquer t dos n participantes possam reconstruir a chave privada.

Em síntese, cada participante utilizar-se-á de um esquema de limiar para compartilhar, entre os $n-1$ participantes, o seu valor x_i;

5. P_i escolhe de maneira aleatória um polinômio $f_i(z)$ de grau $t-1$ sendo que o coeficiente a_0 deste polinômio é a representação numérica de x_i:

$$f_i(z) = x_i + \sum_{j=1}^{t-1} (a_i)_j \, z^j \ (mod\, p)$$

6. P_i então calcula $(F_i)_j = g^{(a_i)_j} \ (mod\, p)$, sendo $j = 1, ..., t-1$, e em seguida publica os valores $(F_i)_j$. $(F_i)_0$ não é calculado pois $(F_i)_0 = g^{x_i} \ (mod\, p) = h_i$ e portanto já é conhecido pelos outros $n-1$ participantes.

   Este procedimento é utilizado para tornar possível a verificabilidade das partes de x_i que serão distribuídas por P_i. Este esquema de verificabilidade é o mesmo apresentado na seção 3.5.1;

7. Após todos terem comprometido estes $t-1$ valores, P_i distribui de maneira secreta, as partes s_{i_k} de x_i, sendo $k = 1, ..., n$ e $k \neq i$:

$$(s_i)_k = f_i(k) = x_i + \sum_{j=1}^{t-1} (a_i)_j k^j \ (mod\, p)$$

   Em particular P_i calcula e guarda para si $(s_i)_i$.

8. A verificabilidade da parte $(s_i)_k$ distribuída pelo participante P_i ao participante P_k é feita através da seguinte equação:

$$g^{(s_i)_k} = h_i \prod_{j=1}^{t-1} (F_i)_j^{k^j} \ (mod\, p)$$

   Se a igualdade não for constatada, significa que ocorreu um erro na parte distribuída por P_i. Neste caso, P_k publica s_{i_k} e interrompe o esquema;

9. Se a verificabilidade das partes ocorrer com sucesso para todos os participantes, cada um deles possuirá uma parte s_i da chave privada x. Esta parte é calculada através da soma das partes $(s_k)_i$ recebidas dos outros $n-1$ participantes com a parte $(s_i)_i$:

$$s_i = (s_i)_i + \sum_{k=1,\ k \neq i}^{n} (s_k)_i \ (mod\ p)$$

10. A partir do momento em que todos os participantes possuírem as partes da chave privada, cada um deles assina sobre a chave pública que é então enviada para uma Autoridade Certificadora (seção 2.5) que por sua vez verifica se as assinaturas de todos os participantes do grupo estão corretas. Caso estejam, ela emite um certificado de chave pública declarando que h é a chave pública daquele grupo;

11. Por fim, quando os participantes do grupo desejarem utilizar a chave privada, basta que eles reúnam-se em um grupo de pelo menos t participantes e reconstruam a chave privada a partir das partes obtidas no passo 9 e utilizando-se da fórmula de Interpolação de Lagrange;

Outro trabalho que trata da criação compartilhada de chaves assimétricas foi apresentado por Dan Boneh e Matthew Franklin em [BON 01]. A proposta consiste em técnicas para a construção compartilhada de pares de chaves aplicáveis ao algoritmo de chave assimétrica RSA.

3.7 Utilização Comercial

O programa PGP (*Pretty Good Privacy*) [NA 01], o qual provê serviços de confidencialidade e autenticação com base em recursos de criptografia, é um exemplo do uso comercial de esquemas de compartilhamento de segredos. Estes esquemas são utilizados pelo PGP no compartilhamento de chaves criptográficas.

Através do serviço de compartilhamento, o PGP permite ao proprietário de uma chave determinar as pessoas a quem ele deseja entregar partes da chave, o número

de partes que deseja entregar a cada uma delas e o número de partes necessárias para a reconstrução da chave (*o limiar do esquema de compartilhamento*).

Na criação e distribuição das partes, cada uma delas é personificada através da sua cifragem com a chave pública ou com um código pessoal do seu respectivo destinatário.

No momento em que se fizer necessária, a reconstrução da chave compartilhada pode ser realizada de duas maneiras: $i)$ *reconstrução local* onde todos os detentores das partes daquela chave encontram-se em um mesmo local; $ii)$ *reconstrução remota* onde os detentores das partes encontram-se separados fisicamente uns dos outros.

A reconstrução local exige a presença física dos detentores das partes para que eles insiram suas partes no computador onde será realizada a decifragem, a fim de possibilitar a sua utilização no algoritmo de reconstrução;

A reconstrução remota exige que os detentores das partes decifrem-nas antes de transmiti-las, através de uma rede de comunicação, ao computador onde a chave será reconstruída. A segurança e confidencialidade da parte durante a transmissão é assegurada pelo protocolo TLS (*Transport Layer Security*), utilizado pelo PGP.

3.8 Conclusão

Existe uma extensa bibliografia relativa a técnicas de compartilhamento de segredos. Este capítulo conceituou apenas as técnicas relevantes às soluções apresentadas nos capítulos 6 e 7, pois a maioria faz uso de esquemas de compartilhamento de segredos. Destaca-se o conteúdo deste capítulo como item essencial para a composição das propostas apresentadas por este trabalho.

Capítulo 4

Criptografia Temporal

4.1 Introdução

Esquemas de criptografia temporal permitem a uma pessoa determinar o momento no futuro em que uma informação eletrônica poderá ser acessada. A garantia da confidencialidade da informação durante seu período de ocultação é garantida pela cifragem de seus dados.

O conceito de criptografia temporal é muito recente, existindo poucos trabalhos abordando o assunto. Porém possuem uma gama de aplicações que justificam sua empregabilidade.

A seção 4.2 introduz os conceitos relativos a esquemas de criptografia temporal. Na seção 4.3 são descritas aplicações em que o uso de esquemas de criptografia temporal é requerido. A seção 4.4 descreve o conceito e o funcionamento de esquemas baseados no uso de quebra-cabeças. A seção 4.5 descreve esquemas baseados no uso de entidades confiáveis responsáveis por guardar uma informação durante um certo período de tempo.

4.2 Conceitos

O objetivo de esquemas de criptografia temporal é possibilitar que uma "informação seja enviada para o futuro"[MAY 93].

Entende-se por "enviar uma informação para o futuro" como a garantia de que uma informação cifrada somente poderá ser decifrada em uma data futura previamente definida ou após a ocorrência de um determinado evento. O espaço de tempo em que uma informação eletrônica será mantida secreta é definido como *período de ocultação*.

Usualmente, em esquemas de criptografia temporal, a informação a ser protegida é cifrada e a chave criptográfica necessária à sua decifragem é ocultada por métodos que garantem a sua confidencialidade durante o período de ocultação. Estes métodos são [RIV 96]:

Quebra-cabeças computacionais: a informação a ser acessada em um período futuro é transformada em um problema somente possível de resolução se um computador ficar processando-o continuamente durante um certo período de tempo pré-definido;

Entidades confiáveis: entidades que comprometem-se a guardar a informação, ou a estrutura que restringe o acesso a mesma, durante um certo período de tempo.

4.3 Aplicações

Esquemas de criptografia temporal possuem uma vasta gama de aplicações. Algumas delas foram citadas no trabalho Ronald L. Rivest, Adi Shamir e David A. Wagner [RIV 96]:

Licitações Públicas: um licitante envia sua proposta comercial selada e esta somente será aberta em data futura previamente determinada e juntamente com as demais propostas dos outros licitantes;

Depósito legal de chaves criptográficas: o governo de um país, por exemplo, deve ser capaz de acessar o conteúdo de comunicações secretas feitas entre pessoas dentro

do seu território. Desta maneira para alguém utilizar criptografia para comunicar-se, deverá deixar sob a tutela do governo uma parcela da chave criptográfica que utilizará para que, se necessário, o governo seja capaz de recuperar por completo a chave. Utilizando criptografia temporal, é possível permitir que o governo tenha acesso à chave completa somente após transcorrido um prazo estabelecido, o que seria mais justo e evitaria práticas ilícitas tal como o acesso indevido a comunicações particulares por agentes do governo;

Pagamentos eletrônicos: quando as parcelas de uma dívida têm datas de vencimento futura, o devedor pode cifrar o dinheiro eletrônico referente ao pagamento de cada uma das parcelas de acordo com o vencimento. Assim o dinheiro somente será decifrado e então disponível ao credor nas datas de vencimento de cada uma das parcelas da dívida;

Informações Pessoais: uma pessoa deseja ocultar informações pessoais durante um certo período de tempo, como o seu diário por exemplo.

Esta lista de aplicações pode ser estendida com o acréscimo das seguintes aplicações:

Informações Governamentais: as consideradas secretas, segredos de guerra por exemplo, devem ser mantidas em sigilo por um determinado período de tempo;

Testamentos: devem ter seu conteúdo revelado somente após a morte do testador;

Provas: após elaboradas devem ser mantidas em sigilo até o momento da sua aplicação, a fim de evitar que terceiros tomem conhecimento das questões antes do devido momento.

4.4 Criptografia Temporal e Quebra-cabeças

Para compreendermos o funcionamento de um quebra-cabeça computacional, é útil fazermos uma analogia com o quebra-cabeça do mundo real o qual *"apresenta dificuldades a serem resolvidas pela perspicácia ou por esforço paciente"* [MIC 98],

normalmente realizados manualmente. Um quebra-cabeça computacional também apresenta dificuldades que devem ser resolvidas, porém, não manualmente, e sim por meio de esforço computacional contínuo durante um certo período de tempo.

O espaço de tempo necessário à resolução de um quebra-cabeça computacional é configurável através da estrutura utilizada na sua construção. Devido a esta propriedade, o quebra-cabeça computacional tornou-se útil a esquemas de criptografia temporal, onde ele é construído de maneira que sua solução somente seja encontrada após transcorrido o tempo em que a informação deve ser mantida secreta.

A utilização de computadores poderosos com grande poder de processamento, paralelização ou distribuição do processamento são meios passíveis de serem utilizados para resolver um quebra-cabeça mais rapidamente do que o previsto na sua construção. Isto se tornaria um problema em esquemas de criptografia temporal, pois não seria possível garantir, mediante a existência de tais ameaças, o tempo em que a informação seria mantida oculta.

Estes problemas foram analisados em [RIV 96] por Rivest, Shamir e Wagner, que buscando solucioná-los, projetaram um quebra-cabeça essencialmente seqüencial e que considera a capacidade de processamento à disposição da entidade que irá resolvê-lo. A seqüencialidade do quebra-cabeça anula o efeito da paralelização ou mesmo distribuição do processamento, já a tentativa de inferir o poder computacional disponível a quem resolverá o quebra-cabeça, busca minimizar o impacto do uso de computadores mais rápidos do que o previsto.

4.4.1 Construção do Quebra-cabeça

No esquema de [RIV 96], a ocultação de uma mensagem M durante um período de T *unidades de tempo (ut)*, é realizada através da execução dos seguintes passos:

1. Gera-se um número composto $n = pq$, resultante do produto de dois números primos bastante grandes e escolhidos aleatoriamente;

2. Calcula-se o valor de $\phi(n) = (p-1)(q-1)$;

3. Calcula-se $t = TS$, onde S é o número de exponenciações módulo n por ut, capazes de serem executadas por quem resolverá o quebra-cabeça e T corresponde ao período de ocultação da mensagem;

4. Gera-se uma chave K aplicável ao criptossistema que será utilizado para cifrar a mensagem, por exemplo: DES, RSA, ElGamal. Caso o criptossistema escolhido seja assimétrico então deve-se gerar um par de chaves assimétricas (Ku e Kr). No restante da descrição do esquema será considerada a escolha de um criptossistema simétrico;

5. Cifra-se a mensagem M utilizando a chave K, $C_M = C(M, K)$;

6. Escolhe-se um número aleatório a, onde $1 < a < n$, e cifra-se K através da operação: $C_K = K + a^{2^t} (mod\, n)$.

   Para realizar o cálculo $a^{2^t} (mod\, n)$ de maneira rápida, deve-se calcular $e = 2^t (mod\, \phi(n))$ e então calcular $a^e (mod\, n)$. Esta simplificação é possível com base no *teorema de Euler* [MEN 96, página 69], o qual afirma que quando n é resultado do produto de dois números primos distintos e sendo $a \in Z_p^*$, o expoente da operação $a^{2^t} (mod\, n)$ pode ser reduzido a módulo $\phi(n)$.

Os valores resultantes são (a, t, n, C_M, C_k). Estes valores representarão a estrutura da mensagem M ocultada e devem ser enviados, de maneira segura, ao destinatário da mensagem.

O destinatário receberá os valores citados acima, porém não será capaz de ler a mensagem M, já que ela se encontra cifrada (C_M). Para ter acesso ao conteúdo da mensagem o destinatário deverá antes recuperar a chave K, que também se encontra cifrada (C_K), para que então consiga decifrar a mensagem M.

4.4.2 Resolução do Quebra-cabeça

A resolução de um quebra-cabeça tem por objetivo recuperar a chave de decifragem K, a qual será utilizada na decifragem da mensagem M. A recuperação da chave K é realizada através da equação:

$$K = C_K - a^{2^t} \ (mod\, n)$$

Para resolver a equação acima, primeiramente deve-se calcular o valor da operação $a^{2^t} \ (mod\, n)$. Este valor será encontrado após a realização de t exponenciações modulares ao quadrado, iniciadas com a base a, como demonstrado no exemplo abaixo onde é resolvida a operação $5^{2^9} \ (mod\ 391)$, onde $p = 17$ e $q = 23$:

$$< \ 5^2, \ 25^2, 234^2, \ 16^2, \ 256^2, \ 239^2, \ 35^2, \ 52^2, \ 358^2 \ (mod\ 391) \Rightarrow \ 307 \ >$$

Esta operação poderia ser facilmente computada se o valor de $\phi(n)$ fosse conhecido, desta maneira bastaria que fossem realizados os mesmos cálculos feitos no passo 6 da construção do quebra-cabeça, para que a solução fosse encontrada antes do encerramento do período de ocultação da mensagem. Por este motivo os fatores de n não devem ser informados a quem resolverá o quebra-cabeça.

Após recuperar a chave K, basta que o destinatário a utilize para decifrar C_M e então ter acesso à mensagem M.

$$M = D(C_M, K)$$

Um possível ataque ao esquema, visando resolver o quebra-cabeça antes do tempo determinado, seria encontrar o valor de $\phi(n)$, mas para isso deve-se primeiro conhecer os fatores de n (p e q). Quando n se trata de um número muito grande, sua fatoração torna-se muito difícil, sendo então mais rápido calcular as t exponenciações do que fatorar n.

As figuras 4.1 e 4.2 apresentam um exemplo da utilização deste esquema.

4.4.3 Verificação Estrutural de um Quebra-cabeça

Protocolos que possibilitam a verificação da estrutura de um quebra-cabeça foram apresentados em [MAO 00, MAO 01, BON 00]. Através destes protocolos

Construção do Quebra-Cabeça:

Alice quer enviar uma mensagem *M* para Beto, com um período de ocultação igual à 5 *ut* (*T*) e fará isso por meio dos seguintes passos:

1. Calcula-se *n*:
   Escolha dos fatores de *n*: $p = 19 \;-\; q = 31$
   Cálculo de *n* e $\phi(n)$: $n = pq$ $\qquad$ $\phi(n) = (p - 1)(q - 1)$
   $n = 19 \times 31 = \mathbf{589}$ $\qquad$ $\phi(n) = (19 - 1) \times (31 - 1) = \mathbf{540}$

2. Calcula-se *t*:
   Definição de *S:* $S = 2$ (exponenciações por *unidade de tempo).*
   Calculo de *t*: $t = TS$
   $t = 5 \times 2 = \mathbf{10}$

3. Gera-se as chaves criptográficas *(Alice optou por utilizar o criptossistema de chave pública RSA).*
   Chave Pública (*Ku*) = 23 - Chave Privada (*Kr*) = 47

4. Cifra-se *M* (*M* = 33) utilizando a chave *Ku* = 23 *(cifragem assimétrica)*:
   $C_M = \text{RSA}(33, 23) \rightarrow C_M = 504$

5. Escolhe-se o valor de *a*: $a = \mathbf{2}$.

6. Oculta-se a chave privada *Kr:*
   Cálculo de a^{2^t}: $e = 2^{10} \; (mod\ 540) = \mathbf{484}$
   $b = 2^{484} \; (mod\ 589) = 233$, portanto $\mathbf{a^{2^t} = 233}$
   Ocultação de *Kr*: $C_{Kr} = 47 + 233 \; (mod\ 589)$
   $C_{Kr} = \mathbf{280} \; (mod\ 589)$

Alice envia para Beto os valores resultantes que representam a mensagem M protegida (2, 10, 589, 504, 280).

Figura 4.1: Construção de um quebra-cabeça.

é possível constatar a correta construção de um quebra-cabeça e com isso determinar se após a sua resolução será ou não possível recuperar a informação oculta. Entretanto não é possível provar antecipadamente que a informação oculta é algo relevante ou não.

Em aplicações que utilizam-se de esquemas de criptografia temporal, estes protocolos são úteis para que o emissor de uma determinada informação prove ao seu receptor que, seguindo os passos necessários, ele conseguirá recuperar a informação oculta.

Os protocolos apresentados em [MAO 00, MAO 01, BON 00] fazem

Resolução do Quebra-Cabeça:

Para conseguir ler a mensagem de Alice, Beto deve recuperar a chave *Kr*. Esta recuperação é realizada através da equação:

$$Kr = C_{Kr} - a^{2^t} \pmod{n}$$

Com base nos valores do quebra-cabeça recebidos de Alice, Beto resolve a equação acima da seguinte maneira:

1. Calcula-se $2^{2^{10}}$ *(mod* 589):

$$\begin{aligned}
2^{2^1} &\rightarrow 2^2 = 4 \ (mod\ 589)\\
2^{2^2} &\rightarrow 4^2 = 16 \ (mod\ 589)\\
2^{2^3} &\rightarrow 16^2 = 256 \ (mod\ 589)\\
2^{2^4} &\rightarrow 256^2 = 157 \ (mod\ 589)\\
2^{2^5} &\rightarrow 157^2 = 500 \ (mod\ 589)\\
2^{2^6} &\rightarrow 500^2 = 264 \ (mod\ 589)\\
2^{2^7} &\rightarrow 264^2 = 194 \ (mod\ 589)\\
2^{2^8} &\rightarrow 194^2 = 529 \ (mod\ 589)\\
2^{2^9} &\rightarrow 529^2 = 66 \ (mod\ 589)\\
2^{2^{10}} &\rightarrow 66^2 = \mathbf{233\ (mod\ 589)}
\end{aligned}$$

2. Conhecendo o valor de $2^{2^{10}}$ *(mod* 589), basta que Beto resolva a equação:

$$Kr = 280 - 233 \pmod{589}$$
$$\boldsymbol{Kr = 47}$$

"A partir deste momento Beto pode decifrar a mensagem utilizando a chave Kr".

Figura 4.2: Resolução de um quebra-cabeça.

uso de protocolos de prova de conhecimento zero para atingirem seus objetivos. Estes protocolos baseiam-se no princípio do fornecimento de provas da detenção de determinada informação, sem a revelação deste conteúdo [SCH 96].

4.4.4 Cápsula do Tempo LCS35

Um exemplo prático da aplicação do esquema proposto por Rivest *et al* foi dado na comemoração dos 35 anos de aniversário do Laboratório para Ciência da Computação (LCS) do *Massachusetts Institute of Technology* (MIT) ocorrida em 1999. Para esta comemoração foi construído um quebra-cabeça que deverá demorar 35 anos para ser resolvido [RIV 99]. Este prazo foi escolhido para que a resolução do quebra-cabeça coincida com a comemoração do setuagésimo aniversário do laboratório.

Este quebra-cabeça está mantido em uma cápsula, chamada de *"LCS35*

Time Capsule Crypto-Puzzle”.

A resolução do quebra-cabeça exigirá processamento contínuo durante os 35 anos, sendo que o computador utilizado no serviço será atualizado anualmente para o modelo mais rápido disponível no momento da troca.

Estruturalmente, o quebra-cabeça foi implementado na linguagem de programação Java e está representado pelas variáveis a, t, n e z, sendo z a mensagem cifrada. À exceção do valor de a, os demais valores do quebra-cabeça são números muito grandes, sendo n um número de 616 dígitos e t um número de 14 dígitos. A definição do valor de t foi embasada na lei de Moore a qual faz projeções sobre o crescimento do poder de processamento em anos futuros.

O resultado do quebra-cabeça surgirá após a realização das t exponenciações. O valor resultante será submetido a uma operação de ou-exclusivo (xor) com o valor de z e o resultado será a mensagem protegida durante os 35 anos (aproximadamente).

4.4.5 Vantagens e Desvantagens

Abaixo são descritas as vantagens e desvantagens de esquemas de criptografia temporal que utilizam-se de quebra-cabeças.

Vantagens:

1. Torna desnecessária a existência de uma terceira entidade pois o remetente entrega a mensagem diretamente para o seu destinatário, que então se empenhará em resolver o quebra-cabeça;
2. Considerado seguro pois é inviável encontrar a chave criptográfica ocultada pelo quebra-cabeça sem resolvê-lo.

Desvantagens:

1. É necessário que um computador trabalhe continuamente durante todo o período de ocultação da informação;

2. Falta de exatidão temporal, pois o tempo de resolução do quebra-cabeça estará ligado à velocidade de processamento da máquina utilizada;
3. A ocorrência de um erro não detectado durante o processamento, ocasiona esforço computacional em vão;
4. Vulnerável ao surgimento de novas e mais rápidas tecnologias, podendo ocasionar uma antecipação na resolução do quebra-cabeça;
5. Em muitas situações, torna-se inviável financeiramente manter uma máquina dedicada à resolução de um quebra-cabeça;
6. Inviável para aplicações que exigem tempo absoluto (exemplo: 08:00hs de 10/Março/2003).

4.5 Criptografia Temporal e Entidades Confiáveis

Outro método utilizado em esquemas de criptografia temporal é o baseado em entidades confiáveis, ou seja, a estas são confiados segredos sob a promessa de entrega ou divulgação somente em data futura. Considera-se como segredo a informação que se deseja proteger ou então a estrutura que restringe o acesso a ela, como por exemplo uma chave criptográfica.

Rivest *et al* [RIV 96] apresentaram dois esquemas baseados no uso de entidades confiáveis. O primeiro deles utiliza-se de esquema de compartilhamento de segredos. O segredo é dividido em diversas partes e entregue a várias entidades, as quais somente divulgarão ou entregarão suas parcelas do segredo no devido momento. O segredo será então reconstruído a partir da união destas partes.

O segundo esquema é caracterizado pela criação de diversos pares de chaves assimétricas. Cada entidade, de um conjunto de entidades confiáveis, cria um par de chaves assimétricas. As chaves públicas destes pares são tornadas públicas logo após a sua criação, já as chaves privadas são publicadas em datas futuras determinadas no ato da criação. Desta maneira um usuário pode utilizar-se de uma destas chaves públicas para cifrar sua informação com a garantia de que a decifragem desta informação somente será

possível em determinado tempo futuro.

Uma variante do segundo esquema de Rivest *et al*, citado acima, foi apresentada em [KUD 99] por Michiharu Kudo e Anish Mathuria . Neste trabalho é apresentado um esquema onde uma terceira entidade é responsável por criar pares de chaves assimétricas e relacioná-los às datas de soltura informadas pelos solicitantes. A geração das chaves é feita mediante requisição de um solicitante, na qual é definida a data futura em que a chave privada deverá ser liberada. A entidade gera o par de chaves e envia a chave pública ao solicitante que então a utiliza para cifrar suas informações. A informação cifrada é enviada ao destinatário juntamente com a data de soltura da chave privada. Na data de soltura, o destinatário deverá solicitar à entidade a chave privada correspondente. A entidade somente liberará a chave se a data atual for igual ou superior à data informada pelo solicitante no ato da criação do par de chaves. Um esquema similar a este foi proposto em [CRE 99] por Giovani Di Crescenzo, Rafail Ostrovsky e S. Rajagopalan.

Michiharu Kudo já havia apresentado um esquema muito semelhante a este em [KUD 98], aplicado a leilões onde as ofertas são entregues lacradas (cifradas) e somente podem ser abertas em evento futuro onde todas as propostas entregues são abertas juntas.

4.5.1 Vantagens e Desvantagens

Abaixo são descritas as vantagens e desvantagens de esquemas de criptografia temporal que utilizam-se de entidades confiáveis.

Vantagens

1. Indicados às aplicações que utilizam tempo absoluto;
2. Não requer esforço computacional constante durante o período de ocultação da informação;
3. Não é vulnerável ao surgimento de tecnologias de processamento mais rápidas.

Desvantagens

1. É necessário que a entidade responsável pela guarda das informações possua a confiança de seus usuários;
2. Vulnerável a uma possível corrupção da entidade;
3. Sujeito a ataques contra a entidade, que podem resultar em perda ou comprometimento das informações mantidas sob sua guarda.

4.6 Conclusão

A criptografia temporal é um campo recente e muito promissor dentro da criptografia, devido à sua aplicabilidade em muitas situações que ocorrem no dia-a-dia. Este capítulo apresentou a conceituação de criptografia temporal e descreveu os métodos utilizados para a implementação de protocolos criptográficos.

Os conceitos de criptografia temporal serão empregados nas soluções apresentadas nos capítulos 6 e 7, mais precisamente nos protocolos responsáveis por garantir a confidencialidade de documentos eletrônicos durante um determinado período de tempo. No capítulo 7 estes conceitos serão utilizados para assegurar que uma proposta comercial, entregue por um fornecedor a um comprador, não terá sua confidencialidade violada durante um período de tempo pré-estabelecido entre as partes.

Capítulo 5

Processo de Compra

5.1 Introdução

Compra pode ser definida como a aquisição de produtos, bens ou serviços que são entregues pelo fornecedor ao comprador mediante compensação financeira equivalente. Uma compra não constitui-se de um ato isolado e sim por uma série de procedimentos ordenados e que visam satisfazer às necessidades do comprador. A união destes procedimentos é chamada *processo de compra*.

Processos de compra possuem caráter estratégico para muitas empresas, pois além de movimentarem somas consideráveis de dinheiro, refletem diretamente nos preços, na qualidade dos serviços e produtos oferecidos por elas.

Este capítulo conceitua *processo de compra* e enfatiza a sua abordagem em entidades públicas.

A partir deste capítulo são considerados como participantes principais de um processo de compra o **comprador** e o **fornecedor**. Existem muitas outras entidades atuantes em um processo de compra, por exemplo: correios, instituições financeiras e agências cartorárias, sendo estas consideradas então como **terceiras entidades**.

Nas seções 5.2 e 5.3 são descritos os processos de compra realizados por empresas privadas e públicas, sendo dado maior enfoque às entidades públicas já que estas possuem uma legislação ampla e rica em detalhes que regulamenta os seus processos

de compra. Por fim, a seção 5.4 aborda a importância da manutenção da confidencialidade dos conteúdos de propostas comerciais entregues durante um processo de compra realizado por uma entidade pública.

5.2 Processos de Compra em Empresas Privadas

O comprador Privado é motivado a conduzir seus processos de compra visando, na maioria das vezes, o aumento na margem de lucro, ganho de vantagens competitivas em relação à concorrência, sobreviver no mercado em que está inserido e outros interesses adicionais. Os procedimentos que compõem seus processos de compra são definidos de acordo com suas políticas internas e interesses particulares da empresa, sempre visando o melhor e o mais vantajoso contrato. Esta cautela é justificável, já que em casos onde o processo de compra resulte em prejuízos ou outros resultados indesejados, a empresa pode ter como conseqüências a diminuição da margem de lucro, a impossibilidade de competição, perda de mercado e outras mais.

Desde que não incorra em práticas ilícitas, o comprador privado têm a liberdade de criar os seus próprios tipos de compra já que ele defende apenas os interesses particulares de sua empresa. Daremos destaque a dois destes tipos:

Compra Direta: quando a compra é efetuada diretamente com o fornecedor que melhor convir à empresa, sem uma disputa entre outros fornecedores. Ocorre normalmente quando comprador e fornecedor são parceiros de negócios ou em casos de padronização de produtos onde o comprador deve optar pelo mesmo fornecedor/fabricante de determinado produto;

Recebimento de Propostas: ocorre quando, publicamente, a empresa solicita o envio de propostas a fim de conhecer os preços e condições de venda de potenciais fornecedores e eventualmente contratar com o que mais lhe interessar.

5.3 Processos de Compra em Entidades Públicas

O comprador público é impedido, por força de lei, de conduzir seus processos de compra de maneira alheia aos interesses públicos ou de acordo com procedimentos não amparados por lei.

As empresas e administrações públicas possuem seus processos de compra regulamentados pela Lei n^o 8.666/93, também chamada de Lei de Licitações. Esta lei estabelece as situações em que as compras realizadas por entidades governamentais são ou não realizadas através de processos licitatórios. Em sua redação, a lei 8.666/93 estabelece, dentre outras normas gerais, cinco possíveis modalidades de licitação: **Concorrência**, **Tomada de Preços**, **Carta Convite**, **Concurso** e **Leilão**. Em 2000 foi instituída pela Medida Provisória 2.026/00 a sexta modalidade de licitação denominada **Pregão** que atualmente é regida pela lei n^o 10.520/02.

A Lei 8.666 impõe regras rígidas às licitações a fim de inibir possíveis fraudes realizadas contra as entidades governamentais. Estas regras, no entanto, tornam o processo de compra demorado, excessivamente burocratizado e algumas vezes prejudicial às entidades governamentais, já que a lei não oferece maneiras de flexibilizar os preços inicialmente propostos pelos potenciais fornecedores, exceto na modalidade pregão. Visando uma reforma na Lei 8.666/93 a fim de tornar os processos de contratação pública mais ágeis e vantajosos ao governo, o Ministério do Planejamento submeteu, através de publicação no Diário Oficial da União em 18 de março de 2002, a consulta pública do "Anteprojeto de Lei-Geral de Contratações da Administração Pública"(Lei 8.666/93).

O anteprojeto propõe mudanças procedimentais e a adoção de novas modalidades de licitação em substituição às instituídas na Lei 8.666/93. As novas modalidades de licitação seriam a **Convocação Geral**, a **Cotação Permanente** e a **Seleção Extraordinária**. As modalidades **Pregão** e **Leilão de Bens** seriam mantidas, mas com modificações.

O anteprojeto, que pode vir a se tornar lei, regulamenta apenas os processos de compra e contratação para bens e serviços. A licitações para obras e serviços de engenharia continuariam regulamentadas pela Lei 8.666/93.

5.3.1 Licitação Pública

O processo regulamentador das compras públicas denominado Licitação Pública pode ser conceituado como sendo *"o processo pelo qual o poder público seleciona a melhor proposta para o contrato de seu interesse e se constitui no principal instrumento de realização de outros princípios constitucionais como os da moralidade administrativa e do tratamento isonômico dos eventuais contratantes com o Poder Púbico"* [CIT 99].

Segundo o artigo 3^o da Lei de Licitações, *"a licitação destina-se a garantir a observância do princípio constitucional da isonomia e a selecionar a proposta mais vantajosa para a Administração e será processada e julgada em estrita conformidade com os princípios básicos da legalidade, da impessoalidade, da moralidade, da igualdade, da publicidade, da probidade administrativa, da vinculação ao instrumento convocatório, do julgamento objetivo e dos que lhes são correlatos"*

5.3.2 Princípios Jurídicos

Os princípios jurídicos citados na redação do artigo 3^o da Lei das Licitações possuem grande importância no cenário das compras públicas. É a observância deles que confere aos processos de compras públicas a transparência e legalidade aos olhos da lei e da opinião púbica.

A conceituação destes princípios segue abaixo:

Isonomia: É *"a norma jurídica que recebe e incorpora o valor da igualdade entre os homens"*[NIE 00]. Através deste princípio estabelece-se que nenhum participante do processo licitatório poderá ter tratamento diferenciado, quer seja em seu benefício ou em seu prejuízo;

Legalidade: Este princípio obriga o administrador público a conduzir todo o processo licitatório de acordo com o estabelecido em lei;

Moralidade: Estabelece que a Administração Pública e seus agentes devem atuar conforme os princípios éticos e morais comuns à sociedade;

Igualdade: É *"o princípio impeditivo da discriminação entre os participantes do certame* [1]*, quer através de cláusulas que, no edital ou convite, favoreçam uns em detrimento de outros, quer mediante julgamento faccioso, que desiguale os iguais ou iguale os desiguais"* [MEI 90];

Impessoalidade: A impessoalidade está ligada ao princípio da igualdade, pois existindo iguais condições entre os participantes, o julgamento das propostas não deverá levar em conta nenhum outro fator senão os ditados pela lei e pelo instrumento convocatório;

Publicidade: Este princípio determina que todos os detalhes inerentes ao processo de compra sejam tornados públicos, para que desta forma todos os possíveis interessados tomem conhecimento da existência do processo;

Economicidade: A entidade pública promotora da licitação deve visar sempre a celebração de um contrato economicamente vantajoso;

Probidade Administrativa: Determina que os administradores públicos devem agir de acordo com os preceitos da lei;

Vinculação ao Instrumento Convocatório: Este princípio vincula todo o processo licitatório ao instrumento convocatório, de forma que a condução do processo se dá de acordo com o descrito neste documento. Entende-se por instrumento convocatório o edital ou a carta convite elaborado pela Comissão de Licitação[2];

Julgamento Objetivo: Este princípio assegura o fiel e rigoroso cumprimento daquilo que está colocado no instrumento convocatório, no momento do julgamento das propostas.

---

[1] Certame: Disputa feita entre os licitantes

[2] Comissão de Licitação: comissão criada pela entidade pública com a função de receber, examinar e julgar todos os documentos e procedimentos relativos à licitação.

5.3.3 Tipos de Licitação

As licitações são julgadas com base nos critérios definidos no instrumento convocatório. Um destes critérios é referente ao tipo em que foi enquadrada a licitação. Segundo o $\S 1^o$ do artigo 45, os tipos de licitação são:

De menor preço: é considerado vencedor o licitante que ofertou, pelo menor preço, o objeto descrito no edital;

De melhor técnica: leva em consideração a capacidade técnica do licitante, sendo vencedor o considerado tecnicamente melhor;

De técnica e preço: considera a capacidade técnica do licitante e também o preço que ele ofertou;

De maior lance ou oferta: utilizado em casos de alienação de bens ou concessão de direito real de uso, sendo considerado vencedor aquele que fizer a oferta de maior valor.

5.3.4 Modalidades de Licitações

No artigo 22 a Lei de Licitações estabelece as modalidades de licitações permitidas, sendo elas, concorrência, tomada de preços, convite, concurso e leilão. Na sua redação original em 1993, foi vedada a criação ou combinação de outras modalidades por parte do administrador público, permanecendo apenas estas cinco modalidades até o ano de 2000, quando foi instituída pela Medida Provisória n^o 2.026, de 4 de maio de 2000, a sexta modalidade de licitação denominada Pregão.

A definição e as aplicações de cada uma das seis modalidades existentes, são descritas abaixo:

Concorrência: destina-se às licitações de maior montante econômico e também às compras e alienações de bens imóveis, as concessões de direito real de uso e às licitações internacionais.

A concorrência, além das suas próprias aplicações, também pode ser utilizada nos casos em que couber a Tomada de Preços ou Convite.

Tomada de preços: destinada às licitações de valores mais reduzidos que a concorrência, visando com isso, atribuir à Administração Pública maior agilidade em alcançar seus objetivos, uma vez que são subtraídas algumas formalidades quando comparada à concorrência.

A principal diferença em relação à concorrência é a existência de um cadastro prévio de fornecedores que substitui a fase da habilitação, embora não proíba a participação dos que não fazem parte do cadastro.

Convite: nesta modalidade a administração pública escolhe um mínimo de 3 fornecedores e envia-lhes uma Carta Convite, a qual faz papel de instrumento convocatório, convidando-os a enviarem suas propostas comerciais. A carta convite enviada para os fornecedores previamente selecionados, deve ser publicada a fim de permitir que outros interessados também participem da disputa.

Leilão: é utilizado para a venda de bens móveis, produtos apreendidos ou penhorados e para a alienação de bens imóveis.

Leilão é realizado em sessão pública presidida por um leiloeiro, onde os licitantes fazem lances verbais e sucessivos até que seja declarado o vencedor. O critério de avaliação utilizado em um leilão é sempre o *de maior lance*, sendo declarado vencedor o licitante que oferecer maior valor pelo objeto leiloado.

Pregão: utilizado para a aquisição de bens e serviços comuns, independente do custo do objeto da compra. Sua realização é feita em sessão pública onde os licitantes fazem lances sucessivos até que seja homologado o vencedor. O critério de avaliação é sempre o de *menor preço*.

Os Pregões podem ser realizados em sessão pública onde todos os participantes estão reunidos fisicamente em um local *(Pregão Presencial)* ou através da Internet *(Pregão Eletrônico).*

Concurso: é utilizada para a contratação de trabalho técnico, científico ou artístico.

O enquadramento de um processo licitatório em uma ou outra modalidade se dá pelo valor estimado do objeto da licitação e pela sua natureza, como por exemplo: obras e serviços de engenharia, venda de imóveis, aquisição de produtos. A tabela 5.1 apresenta a aplicabilidade das modalidades de licitação segundo os critérios valor e natureza do objeto.

Tabela 5.1: Aplicabilidade das modalidades quanto ao valor e à natureza do objeto. Valores dados pela Lei 8.666/93 em seu texto atualizado em 20/09/2001 (Texto vigente em 27/08/2002).

Modalidades	**Valor Estimado do Objeto**	**Natureza do Objeto**
Concorrência	Acima de R$ 1.500.000,00	Obras e serviços de engenharia.
	Acima de R$ 650.000,00	Demais compras e contratações de serviços
Tomada de Preço	Até R$ 1.500.000,00	Obras e serviços de engenharia.
	Até R$ 650.000,00	Demais compras e contratações de serviços.
Convite	Até R$ 150.000,00	Obras e serviços de engenharia.
	Até R$ 80.000,00	Demais compras e contratações de serviços.
Leilão	Qualquer valor	Venda de bens móveis, produtos apreendidos ou penhorados e para a alienação de bens imóveis.
Pregão	Qualquer valor	Aquisição de bens e serviços comuns.
Concurso	Qualquer valor	Contratação de trabalho técnico, científico ou artístico.

Em processos licitatórios existe um intervalo de tempo mínimo entre a publicação do instrumento convocatório e a entrega das propostas pelos licitantes ou ocorrência do leilão ou concurso. A tabela 5.2 relaciona estes prazos e em quais circunstâncias eles são exigidos.

5.3.5 Fases do Procedimento Licitatório

De maneira genérica, as fases que compõem uma licitação são equivalentes para todas as modalidades, exceto para a modalidade pregão que, por este motivo será descrita separadamente na seção 5.3.6.

Tabela 5.2: Prazos mínimos decorridos entre a publicação do edital e a entrega de propostas ou realização do evento.

Modalidades	**Prazo Mínimo**	**Circunstâncias**
Concorrência	45 dias	Em contratos celebrados sob o regime de empreitada integral ou em Licitações dos tipos *melhor técnica* ou *técnica e preço*.
	30 dias	Nos demais casos.
Tomada de Preço	30 dias	Licitações do tipo *melhor técnica* ou *técnica e preço*
	15 dias	Nos demais casos.
Convite	5 dias úteis	Todas
Leilão	15 dias	Todas
Pregão	8 dias úteis	Todas
Concurso	45 dias	Todas

Preparação: fase onde se tem início o processo de licitação a partir de abertura de processo administrativo e elaboração do instrumento convocatório. A publicidade da licitação também é feita nesta fase através da publicação do instrumento convocatório nos meios de comunicação devidos.

Habilitação: Nesta fase os interessados em participar da licitação entregam, em envelopes lacrados e separados, a documentação exigida no instrumento convocatório e a sua proposta comercial. Somente é entregue o envelope contendo os documentos para habilitação quando o fornecedor não possuir cadastro prévio.

Os documentos passíveis de exigência são relativos a:

- Habilitação jurídica;
- Qualificação técnica;
- Qualificação econômico-financeira;
- Regularidade fiscal.

Cada um destes tópicos representa uma série de documentos. A descrição detalhada destes documentos encontra-se nos Art. 28, 29, 30, 31, 32 e 33 da Lei 8666/93.

Na data prevista no instrumento convocatório e antes da abertura do envelope de proposta, é realizada a abertura e análise dos documentos de habilitação. Os participantes considerados inabilitados terão seus envelopes de proposta devolvidos ainda lacrados.

Julgamento: nesta fase são abertos os envelopes contendo as propostas dos licitantes considerados habilitados. A conformidade de cada proposta é verificada com os requisitos do instrumento convocatório e então julgada e classificada de acordo com os critérios de avaliação também descritos no instrumento convocatório. Por fim, ocorre a escolha e homologação do vencedor por parte da Comissão de Licitação.

A figura 5.1 ilustra a ordem das fases do processo licitatório.

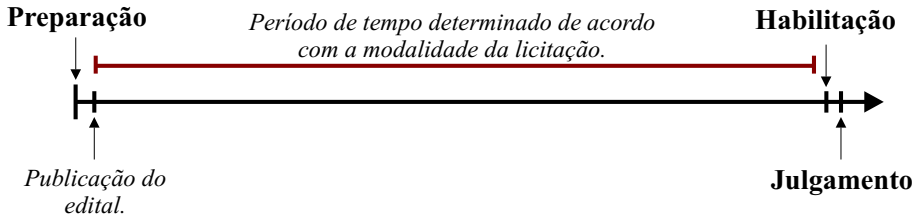

Figura 5.1: Disposição temporal dos procedimentos de um processo licitatório.

5.3.6 Modalidade Pregão

A modalidade pregão possui fases iguais às outras modalidades, mas com procedimentos e ordenação diferentes.

Preparação: nesta fase é justificada a necessidade da licitação, designado o Pregoeiro (pessoa responsável pela condução do Pregão) e a sua equipe de apoio, redigido e publicado o edital (instrumento convocatório).

Julgamento: Inicia com o recebimento dos envelopes contendo as propostas e os documentos de habilitação, prosseguindo com a imediata abertura e classificação do envelope das propostas. O critério de classificação das propostas será sempre o “de menor preço”.

O pregoeiro escolhe a proposta de menor valor e a utiliza como referencial para a escolha de outras propostas cujos valores sejam até 10% superiores ao valor de referência. É constituído um grupo com os licitantes escolhidos e estes poderão fazer novos lances sucessivos baixando os valores das suas propostas iniciais até que seja proclamado um vencedor, mas sempre obedecendo o critério de menor preço.

Habilitação: escolhido o licitante vencedor, o pregoeiro procede com a abertura do envelope onde estão os documentos de habilitação do licitante para a devida avaliação. Caso o licitante não seja considerado habilitado, é escolhida a segunda melhor proposta e então verificada a documentação de quem a submeteu, assim sucessivamente até que um dos licitantes escolhidos seja considerado habilitado.

A figura 5.2 ilustra a ordem em que as fases do processo licitatório da modalidade pregão ocorrem.

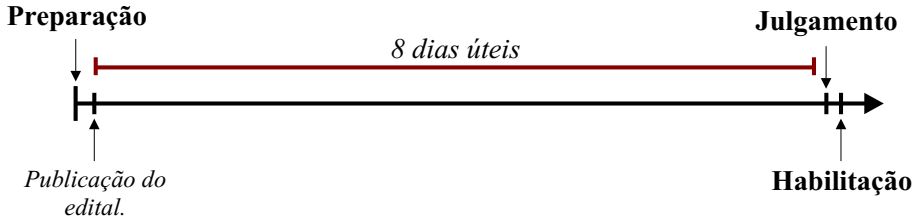

Figura 5.2: Disposição temporal das fases de um processo licitatório (Modalidade Pregão).

Tanto o pregão eletrônico quanto o presencial, utilizam-se destas mesmas fases, mudando apenas o meio sobre o qual são realizadas, sendo no eletrônico através do portal de compras do Governo Federal, o Comprasnet[3], e o presencial através da reunião física dos licitantes em um determinado local.

Podemos destacar aqui algumas das características que diferem o pregão das demais modalidades:

- Inexistência de limite de valores;

[3]www.comprasnet.gov.br

- Alternativa às modalidades Concorrência, Tomada de Preços e Convite;
- Utilização de recursos de tecnologia da informação;
- Inversão das fases de habilitação e classificação dos licitantes;
- Menor prazo exigido entre a publicação do edital e a ocorrência do pregão. Isto deu ao governo maior agilidade em seus processos de compra.
- Aumento de competitividade, permitindo o ajuste das propostas inicialmente feitas pelos participantes;
- Redução de custos pois permite a redução dos preços ofertados inicialmente.

5.3.7 Dispensa e Inexigibilidade da Licitação Pública

A Licitação Púbica é regra obrigatória para a contratação de fornecedores pelos órgãos governamentais, porém existem exceções onde o processo licitatório é dispensável ou inexigível. Concede-se com isso a permissão à Administração Pública para efetuar compras diretamente com o fornecedor que lhe for mais conveniente, sem que para isso seja necessário passar por toda a parte burocrática que compõe um processo licitatório.

Os casos em que o processo licitatório é dispensável são descritos pela Lei 8.666/93 nos seus artigos 17 ($\S\S$ 2^o e $\S\S 4^o$) e 24. Alguns destes casos são:

- Para obras e serviços de engenharia de valor até R$ 15.000,00 (quinze mil reais);
- Para outros serviços e compras de valor até R$ 8.000,00 (oito mil reais);
- Nos casos de emergência ou de calamidade pública;
- Quando a União tiver que intervir no domínio econômico para regular preços ou normalizar o abastecimento;
- Nas compras de hortifrutigranjeiros, pão e outros gêneros perecíveis;

Já os casos que representam a inexigibilidade da Licitação Pública, estão descritos no artigo 25 da mesma lei. São eles:

- Para aquisição de materiais, equipamentos, ou gêneros que só possam ser fornecidos por produtor, empresa ou representante comercial exclusivo;
- Para a contratação de serviços técnicos de natureza singular, com profissionais ou empresas de notória especialização;
- Para contratação de profissional de qualquer setor artístico, desde que consagrado pela crítica especializada ou pela opinião pública.

5.4 Confidencialidade das Propostas Comerciais

Nos processos de compra públicos que envolvem licitação, as propostas comerciais são entregues em envelopes lacrados que só poderão ser abertos em evento público previamente determinado no instrumento convocatório. Este procedimento é obrigatório por lei e está estabelecido na lei 8.666/93 em seu artigo 3^o, § 3^o, onde é dito:

> *"A licitação não será sigilosa, sendo públicos e acessíveis ao público os atos de seu procedimento, salvo quanto ao conteúdo das propostas, até a respectiva abertura"*.

Fica clara na redação dada pela lei que o conteúdo das propostas não poderá ter sua confidencialidade violada até que chegue a data onde todas as propostas serão abertas juntas e em sessão pública. A lei é rigorosa em casos onde o disposto no artigo 3^o, § 3^o não é respeitado. O artigo 94 desta mesma lei diz:

> *"Devassar o sigilo de proposta apresentada em procedimento licitatório, ou proporcionar a terceiro o ensejo de devassá-lo:* ***Pena*** *- detenção, de 2 (dois) a 3 (três) anos, e multa."*

As empresas privadas, por possuírem maior liberdade, podem utilizar-se dos mecanismos criados pelas leis que regem as licitações públicas na constituição de seus processos de compra, tais como manter o sigilo das propostas por um determinado tempo e penalizar quem tenta fraudar o processo através da violação dos envelopes. No entanto as penalizações descritas nesta lei não se aplicam em processos de compra de empresas privadas, cabendo a estas buscar outros meios legais de punição àqueles que desrespeitarem as regras de seus processos de compra.

5.5 Conclusão

Este capítulo apresentou a conceituação e o funcionamento de processos de compra bem como suas diferentes abordagens dentro de entidades públicas e privadas. Também foi mostrada a importância dada aos envelopes que contêem as propostas comerciais submetidas à avaliação do comprador, sendo de suma importância que seja garantida a confidencialidade e inviolabilidade destas até determinado evento futuro e que neste evento seja possível abrir todas as propostas entregues.

Capítulo 6

Protocolos de Criptografia Temporal em Grupos

6.1 Introdução

A possibilidade de determinar o momento futuro em que uma informação eletrônica poderá ser acessada, contemplada pela criptografia temporal, é requisito necessário a muitas aplicações, as quais já foram em parte citadas nos capítulos anteriores deste trabalho.

A criação de protocolos criptográficos eficazes no campo da criptografia temporal é de grande valia e justificada pelo número de aplicações onde eles podem ser empregados.

Este capítulo apresenta novos protocolos criptográficos que se propõem a permitir que seja determinada, no ato da cifragem de uma informação, a data futura em que esta poderá ser decifrada. Estes protocolos dão ênfase à necessidade de se assegurar que na data determinada, a informação poderá ser decifrada independente da vontade de quem a cifrou.

Os protocolos propostos neste capítulo visam, em especial, prover serviços de criptografia temporal para grupos de entidades.

A seção 6.2 apresenta uma visão geral dos protocolos propostos, des-

tacando seus objetivos e os métodos utilizados. Na seção 6.3 são apresentados dois protocolos, os quais propõem a construção e o uso de módulos criptográficos de hardware em esquemas de criptografia temporal. A seção 6.4 apresenta quatro protocolos que destinam-se especificamente a prover serviços de criptografia temporal a grupos de usuários, utilizando esquemas de compartilhamento de segredos. Por fim, a seção 6.5 apresenta uma análise da segurança oferecida pelos protocolos propostos.

6.2 Visão Geral

Os **protocolos de criptografia temporal em grupos** se propõem a assegurar, através de técnicas de criptografia, a confidencialidade de um documento eletrônico durante um determinado período de tempo. Após expirado este período, os protocolos devem assegurar que a decifragem deste documento seja permitida mesmo contra a vontade de quem o cifrou. O espaço de tempo em que o documento eletrônico deve ser mantido secreto é determinado no momento da sua cifragem.

Assim como nos protocolos de criptografia temporal descritos no capítulo 4, os protocolos de criptografia temporal em grupos ocultam a chave criptográfica necessária à decifragem de um documento, durante o período em que se deseja manter secreto o seu conteúdo e com isso asseguram a confidencialidade deste documento durante o tempo desejado.

Neste capítulo são propostos seis novos protocolos destinados a prover serviços de criptografia temporal. Os protocolos propostos são divididos em duas seções, 6.3 e 6.4, de acordo com os métodos que eles adotam para ocultar a chave criptográfica de decifragem necessária à decifragem de um documento e em relação às restrições quanto às entidades que podem fazer uso dos protocolos.

6.3 Protocolos Baseados em Módulos Criptográficos de Hardware

Nesta seção são propostos dois novos protocolos de criptografia temporal, os quais são baseados no uso de módulos criptográficos de hardware no gerenciamento de chaves criptográficas. Estes módulos são os responsáveis pela manutenção da confidencialidade de documentos eletrônicos, assegurando que as chaves criptográficas necessárias à decifragem destes documentos não serão divulgadas antes do tempo previamente determinado.

Estes protocolos não são exclusivos para a prestação de serviços de criptografia temporal a grupos, pois podem prover também estes serviços de maneira individual.

6.3.1 Notação

Na descrição destes protocolos é utilizada a seguinte notação:

AC : Autoridade Certificadora;

DP : Diretório Público. Local onde são publicadas informações que devem estar acessíveis a todos;

T : período de tempo em que o conteúdo de um documento cifrado deve permanecer secreto;

TKr : chave privada que deve ser mantida secreta durante o período de tempo *T*;

TKu : chave pública correspondente a *TKr*;

R(TKu) : resumo da chave *TKu*;

REQ( ) : requisição enviada a uma terceira entidade responsável pela criação das chaves *TKr* e *TKu*.

6.3.2 Protocolo MCH-1

Este protocolo considera a construção de um módulo criptográfico de hardware, o **MCH-1**, que oferece serviços de criação e proteção de chaves criptográficas.

O funcionamento do MCH-1 consiste em criar, mediante requisições de usuários, pares de chaves assimétricas (*TKr* e *TKu*), divulgar as chaves públicas destes pares e proteger contra a divulgação as chaves privadas. Estas são mantidas sob proteção do MCH-1 até as *datas de divulgação* determinadas pelos usuários. As chaves públicas criadas pelo MCH-1 são todas certificadas digitalmente por uma autoridade certificadora, que informa no campo de extensão de cada certificado a data em que ocorrerá a divulgação da respectiva chave privada.

A data de divulgação de uma chave privada é informada na requisição enviada ao módulo. Esta requisição também deve conter um ou mais códigos secretos utilizados para personificar a entrega da chave privada. Considerando o atendimento a grupos de entidades, uma requisição pode conter mais de um código secreto, o que permite que o grupo escolha um ou mais líderes para responsabilizarem-se pela liberação da chave privada. A personificação é alcançada pois estes códigos devem ser novamente inseridos para que a liberação da chave ocorra. Os códigos secretos informados na requisição devem estar cifrados com a chave pública do MCH-1, o que garante a sua confidencialidade.

Portanto, a divulgação de uma chave privada, mantida sob a proteção do MCH-1, somente ocorre se forem satisfeitos dois requisitos de segurança:

1. **Temporalidade:** a data atual deve ser igual ou superior a data de divulgação informada na requisição;

2. **Autenticação:** a liberação somente ocorre mediante a inserção dos códigos secretos informados na requisição.

O MCH-1 utiliza um relógio interno para obter o tempo sobre o qual baseia suas ações. Considerando a natureza temporal crítica dos serviços prestados pelo MCH-1, é fundamental que este obtenha de maneira confiável o tempo. Isto é alcançado através da sincronização segura do seu relógio interno com uma fonte confiável de tempo.

A entidade responsável por gerar e disseminar a hora legal brasileira, sendo portanto exemplo de uma fonte confiável de tempo, é o Observatório Nacional brasileiro [Dec]. O processo de sincronização segura de relógios é descrito por Dias *et al* em [DIA 03].

O requisito autenticação pode ser considerado facultativo, podendo ser delegado o poder de escolha ao usuário, devendo este informar a exigência de tal requisito na requisição enviada ao módulo, ou fazer parte da configuração do MCH-1. Entretanto, o restante da descrição deste protocolo considera a exigência de ambos os requisitos para a liberação de uma chave *TKr*.

Abaixo são descritos os passos que compreendem a criação de um par de chaves *TKr* e *TKu* através do MCH-1, considerando como solicitante do serviço um grupo de indivíduos, embora o serviço oferecido pelo MCH-1 não é restrito a grupos, podendo também ser utilizado por um único indivíduo. :

1. Os líderes do grupo criam uma requisição contendo uma data de divulgação e o código secreto de cada um dos líderes, cifrados pela chave pública do MCH-1;
2. O MCH-1 cria o par de chaves, *TKr* e *TKu*;
3. O MCH-1 calcula o resumo da chave *TKu* e o utiliza na identificação segura do par de chaves;
4. O MCH-1 armazena internamente a chave *TKr*, vinculada ao resumo da chave *TKu*, à data de divulgação e aos códigos secretos informados;
5. O MCH-1 envia à Autoridade Certificadora a chave *TKu*, a data de divulgação e o resumo da chave *TKu*;
6. A Autoridade Certificadora gera o certificado digital e o envia ao MCH-1. No campo de extensão do certificado são declarados a data de divulgação da chave *TKr* e o resumo calculado pelo MCH-1;
7. O MCH-1 envia aos líderes do grupo o certificado digital.

Abaixo são descritos os passos que compreendem a divulgação de uma chave *TKr* mantida sob a proteção do MCH-1:

1. Os líderes do grupo informam ao módulo o resumo contido no certificado digital e os códigos secretos informados no passo 2 da criação das chaves;

2. Através do resumo informado o MCH-1 localiza a chave *TKr* solicitada;

3. O MCH-1 verifica o atendimento do requisito autenticação comparando os códigos informados no passo 1 com os códigos vinculados à chave *TKr*;

4. O MCH-1 verifica o atendimento do requisito temporalidade comparando o tempo atual, que consta no seu relógio interno, com a data de divulgação vinculada à chave *TKr*;

5. Se ambos os requisitos forem satisfeitos, o módulo envia aos líderes a chave *TKr*.

Estes passos garantem essencialmente que uma chave *TKr* não será liberada antes da data definida na requisição que a originou, e que ela será entregue somente a pessoas autorizadas, ou seja, aos portadores dos códigos informados na requisição.

A interação entre as entidades componentes do protocolo, nos momentos da criação de um par de chaves *TKr* e *TKu* e da divulgação da chave *TKr*, é demonstrada na figura 6.1.

O projeto e a implementação do MCH-1 devem satisfazer requisitos de segurança estabelecidos por órgãos competentes, tal como o FIPS PUB[1] 140-2 do Instituto Nacional de Padrões e Tecnologia americano (NIST), o qual especificou tais requisitos em [NIS 01b]. Esta prática se faz necessária devido à natureza crítica das informações que são mantidas pelo MCH-1.

6.3.3 Protocolo MCH-2

Este protocolo também considera a construção de um módulo criptográfico de hardware, o qual oferece serviços de criação e proteção de chaves criptográficas.

[1] *Federal Information Processing Standards Publication*

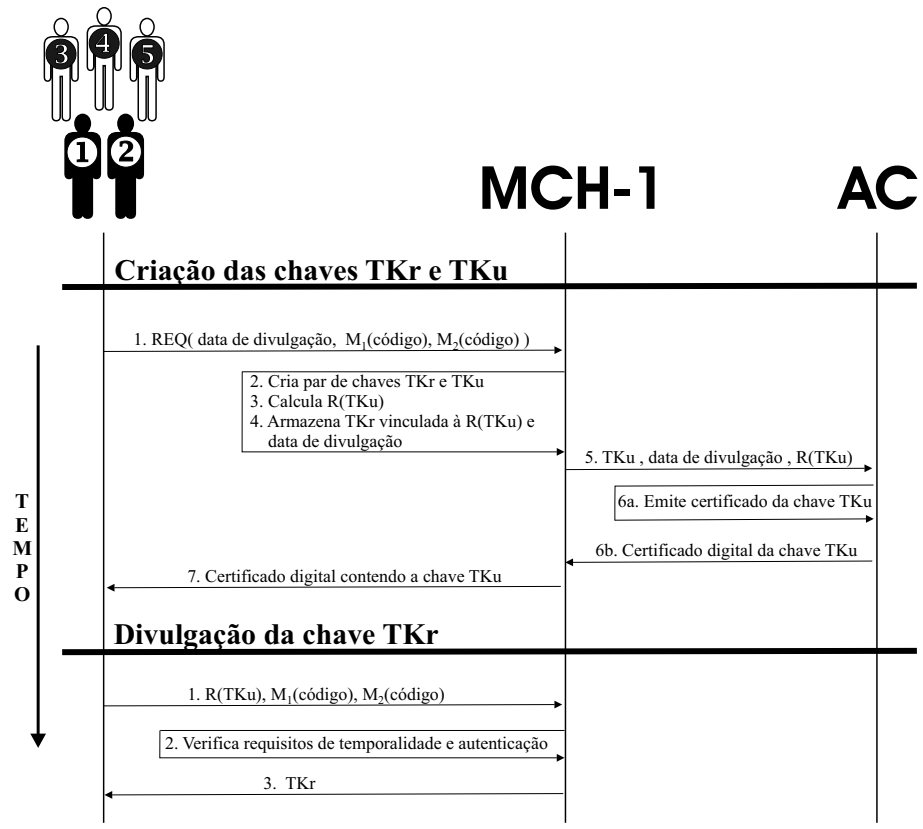

Figura 6.1: Protocolo MCH-1: Os líderes do grupo são apresentados em destaque pelos membros identificados por 1 e 2. Os momentos de criação do par de chaves *TKr* e *TKu* e de divulgação da chave *TKr* são descritos através dos fluxos separados pelas linhas horizontais que percorrem toda a figura. A linha vertical representativa do tempo indica a seqüência em que os passos são executados.

O funcionamento deste módulo, denominado **MCH-2**, consiste na geração de uma seqüência grande de pares de chaves assimétricas (*TKr* e *TKu*) . As chaves públicas destes pares são publicadas logo após a sua criação, já as chaves privadas são publicadas, uma após a outra, em datas futuras determinadas pelo MCH-2 no momento da sua criação.

Logo após a criação da seqüência de chaves, o MCH-2 envia todas as chaves públicas (*TKu*) a uma Autoridade Certificadora para a emissão de certificados digitais. No campo de extensão de cada um dos certificados, consta a data de publicação da respectiva chave privada (*TKr*). Estes certificados são devolvidos ao MCH-2 que por sua vez publica-os no *DP*.

A publicação das chaves *TKr* deve ocorrer na mesma seqüência em que elas foram criadas e somente nas datas previamente determinadas. A fim de garantir a seqüencialidade na publicação, cada chave *TKr* é ligada a sua antecessora. Com isto o conhecimento de uma chave está condicionado ao conhecimento prévio da sua antecessora. Este encadeamento de chaves torna a segurança do MCH-2 mais robusta, uma vez que um agente malicioso não pode empreender um ataque ao módulo objetivando comprometer a segurança de uma única chave *TKr*.

A ligação entre as chaves é feita no momento da criação da seqüência de chaves e consiste em cifrar a chave *TKr* do par atual com a chave *TKu* do par anterior. Desta maneira uma chave *TKr* somente será conhecida após a sua decifragem, o que exigirá a chave *TKr* do par anterior.

A utilização dos serviços do MCH-2 não requer qualquer interação do usuário com o módulo. Para proteger um documento eletrônico durante um período de tempo *T*, basta que o usuário verifique no *DP* qual é a chave *TKu* que possui a sua chave *TKr* divulgada na data desejada e então utilizá-la na cifragem do documento.

O tempo utilizado pelo MCH-2 é obtido da mesma maneira que é obtido pelo MCH-1, ou seja, através da sincronização segura do seu relógio interno com uma fonte confiável de tempo.

A figura 6.2 ilustra o funcionamento do protocolo e a interação entre as entidades que o compõem, considerando como usuário do serviço um grupo de indivíduos. O serviço oferecido pelo MCH-2 não é restrito a grupos, podendo também ser utilizado por um único indivíduo.

Esta proposta é similar a apresentada por Ronald L. Rivest, Adi Shamir e David A. Wagner em [RIV 96]. A diferença em relação a esta proposta é a adoção de uma única entidade na criação e proteção dos pares de chaves, enquanto que Rivest *et al* prevêem a utilização de várias entidades, onde cada uma delas cria um par de chaves e se responsabiliza por divulgar a chave privada daquele par somente em uma determinada data futura. Outro diferencial é o encadeamento das chaves, inexistente na proposta de Rivest *et al*. Tais características adicionais tornam o protocolo MCH-2 mais robusto que o apresentado em [RIV 96].

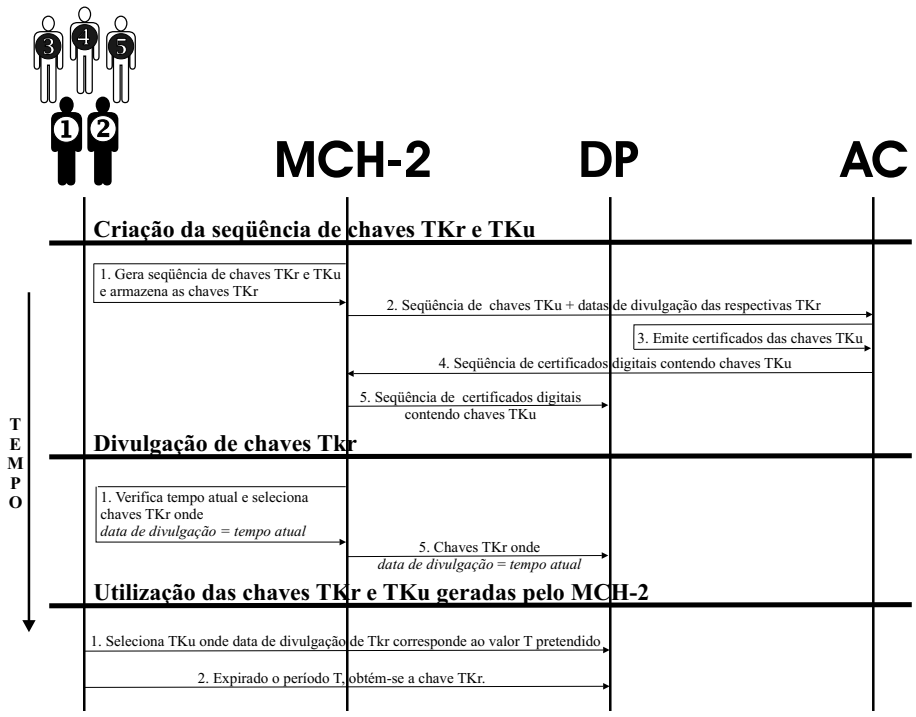

Figura 6.2: Protocolo MCH-2: Os líderes do grupo são apresentados em destaque pelos membros identificados por 1 e 2. Os fluxos separados pelas linhas horizontais que percorrem a figura descrevem as diferentes fases que compõe o protocolo. A linha vertical representativa do tempo indica a seqüência em que os passos são executados.

Assim como no protocolo MCH-1, o projeto e a implementação do módulo MCH-2 também devem satisfazer requisitos de segurança estabelecidos por órgãos competentes devido à natureza crítica das informações que mantém.

6.4 Protocolos Baseados em Compartilhamento de Segredos

Os protocolos baseados em esquemas de compartilhamento de segredos destinam-se especificamente a prover serviços de criptografia temporal para grupos em que seus membros possuem interesses comuns. A criação de um grupo consiste em reunir entidades que desejam garantir a confidencialidade de um ou mais documentos eletrônicos de uma mesma natureza e pelo mesmo período de tempo. Documentos de uma mesma

natureza dizem respeito a documentos empregados com um mesmo propósito, como por exemplo, propostas comerciais entregues em um processo de licitação pública.

Estes protocolos prevêem o envio de documentos eletrônicos apenas entre membros de um mesmo grupo. Desta maneira, quando o membro *A* emite um documento *D* e o envia cifrado ao membro *B*, é assegurado a *A* que *B* não consegue decifrar *D* antes da expiração do período de tempo *T*, determinado no ato da cifragem. É também assegurado a *B* que a decifragem de *D* é possível após a expiração de *T* independentemente da vontade de *A*, porém não da dos demais membros do grupo.

Estes protocolos possuem duas premissas básicas: igualdade de interesses e solidariedade em relação aos malefícios causados a um ou mais membros do grupo.

A igualdade de interesses traduz-se na necessidade que os membros do grupo possuem de garantir a documentos eletrônicos, de uma mesma natureza e emitidos pelos próprios membros, a sua confidencialidade durante um mesmo período de tempo. Enquanto a solidariedade em relação aos malefícios causados a membros do grupo refere-se ao fato que se um membro prejudicar um outro membro do mesmo grupo, ele também será prejudicado e na mesma proporção. Através destas premissas as entidades são levadas a respeitar as etapas e regras dos protocolos.

O funcionamento dos protocolos consiste na interação entre os indivíduos membros de um mesmo grupo em esquemas de compartilhamento de segredos. A interação também ocorre com entidades externas ao grupo na condição de prestadoras de serviços ao grupo, como por exemplo uma Autoridade Certificadora que presta serviços de certificação digital.

A adoção de esquemas de compartilhamento de segredos busca transferir a responsabilidade da confidencialidade dos documentos eletrônicos para os próprios membros do grupo, utilizando o conceito de *confiança distribuída*. Nestes protocolos a chave criptográfica necessária à decifragem de um ou mais documentos eletrônicos (*TKr*) é dispersa entre os indivíduos membros do grupo, tornando-os responsáveis pela manutenção da confidencialidade destes documentos durante um período previamente determinado.

O compartilhamento da chave *TKr* é realizado através do esquema de

Shamir, conceituado na seção 3.4.1. As figuras 6.3 e 6.4 apresentam respectivamente os protocolos de construção e reconstrução contidos no esquema de Shamir e que serão utilizados, respectivamente, para **quebrar**[2] e reconstruir a chave *TKr*. Os protocolos descritos nas figuras encontram-se adaptados ao contexto dos protocolos propostos neste capítulo.

Esquema de Shamir: Protocolo de Construção

1. São definidos os parâmetros t e n, sendo:
   - n: número total de membros entre os quais será dividida a chave *TKr*;
   - t: limiar do esquema.

2. Escolhe-se um número primo p de maneira aleatória, respeitando a condição que exige que p seja maior que n e *TKr*;

3. Cria-se um polinômio $f(x)$ a partir de coeficientes escolhidos randomicamente, com exceção ao coeficiente a_o o qual representará o valor de *TKr*:

$$f(x) = TKr + \sum_{j=1}^{t-1} a_j x^j \ (mod\ p)$$

4. Gera-se as partes TKr_i submetendo ao polinômio $f(x)$ os valores de x_i, os quais representam os identificadores numéricos ($i = 1, \ldots, n$) de cada membro do grupo:

$$TKr_i = f(x_i)$$

Figura 6.3: Esquema de Shamir - Protocolo de Construção: Através deste protocolo são geradas as partes da chave *TKr*.

O protocolo de distribuição, compreendido entre os protocolos de construção e reconstrução, trata da distribuição das partes geradas com a quebra da chave *TKr* aos participantes do esquema. O envio das partes da chave deve ser realizado de maneira segura, utilizando canais de comunicação privados entre quem compartilha e quem recebe partes da chave, ou utilizando criptografia assimétrica cifrando as partes da chave *TKr* com as chaves públicas dos respectivos destinatários.

Para prevenir um eventual envio de partes inconsistentes, tanto no protocolo de distribuição quanto no protocolo de reconstrução, é adotado um esquema de verificabilidade de compartilhamento, o qual acusará a incorreção em uma ou mais partes

[2]Quebrar: termo utilizado para transmitir a idéia da separação de um todo em partes, retratando desta maneira a idéia contida nos esquemas de compartilhamento de segredos onde divide-se um determinado segredo em diversas partes.

Esquema de Shamir: Protocolo de Reconstrução

1. *t* dos *n* participantes do esquema devem revelar as suas partes TKr_i da chave *TKr*;

2. Conhecendo-se *t* partes de *TKr*, deve ser usada a fórmula de interpolação de *Lagrange* para reconstruir a chave *TKr*:

$$TKr = \sum_{j=1}^{t} b_j \, TKr_{i_j} \qquad \text{onde} \qquad b_j = \prod_{1 \le k \le t,\, k \ne j} \frac{x_{i_k}}{x_{i_k} - x_{i_j}}$$

Figura 6.4: Esquema de Shamir - Protocolo de Reconstrução: Este protocolo possibilita a reconstrução da chave *TKr* com base em um número mínimo de partes geradas no protocolo de construção.

do segredo quando e se ela ocorrer. Os esquemas de verificabilidade estudados permitem somente validar as partes de um segredo enviadas por uma entidade no sentido de garantir a integridade e procedência destas partes. No entanto, não é possível garantir através destes esquemas que um determinado segredo compartilhado é ou não o que se espera que ele seja. O esquema de verificabilidade adotado nos protocolos de criptografia temporal em grupos baseados em compartilhamento de segredos é o apresentado por Markus Stadler em [STA 96], descrito na seção 3.5.1 e que pode ser visto nas figuras 6.5 e 6.6.

Esquema de Stadler: Protocolo de Construção

1. Quebra-se a chave *TKr* utilizando o protocolo de construção do esquema de Shamir;

2. Escolhe-se um número gerador *g* pertencente ao conjunto Z_p^* (conjunto gerado através do número primo *p* utilizado no esquema de Shamir);

3. Utilizando os coeficientes do polinômio *f(x)* criado no passo 1, calcula-se os seguintes valores:

$$S = g^{TKr} \;\; e \;\; A_j = g^{a_j} \;\; (sendo\ j = 1, \ldots, t\text{-}1)$$

4. Publica-se no *DP* os valores de *g, S* e A_j relacionados a um dado identificador da chave *TKr*.

Figura 6.5: Esquema de Verificabilidade - Protocolo de Construção: Neste protocolo são calculados e publicados os valores de comprometimento g, S e A_j.

Esquema de Stadler: Protocolo de Verificação

1. Cada parte TKr_i é enviada ao membro M_i, sendo $i = 1, \ldots, n$;

2. Cada membro M_i verifica a integridade da sua própria parte TKr_i através da seguinte equação:

$$S_i = S \prod_{j=1}^{t-1} A_j^{x_i^j}$$

A parte TKr_i somente deve ser considerada correta se satisfizer à equação:

$$S_i = g^{TKr_i}$$

3. Se o resultado for positivo, M_i informa a todos através do envio de uma mensagem de aceitação, caso contrário envia uma mensagem de rejeição, encerrando o protocolo em seguida.

Figura 6.6: Esquema de Verificabilidade - Protocolo de Verificação: Este protocolo permite o destinatário de uma parte da chave *TKr* constatar a integridade da parte recebida.

6.4.1 Notação

Na descrição dos protocolos baseados em esquemas de compartilhamento de segredos são utilizados, além dos símbolos definidos na seção 6.3.1, os seguintes símbolos:

t : limiar do esquema de Shamir;

n : número total de membros entre os quais será dividida a chave *TKr*;

$\boldsymbol{M_i}$: membro i de um grupo;

$\boldsymbol{TKr_i}$: parte da chave *TKr* gerada através do esquema de Shamir;

$\boldsymbol{M_i TKr}$: chave *TKr* pertencente a M_i;

$\boldsymbol{M_i TKr_j}$: parte j da chave *TKr* pertencente a M_i, gerada através do esquema de Shamir.

6.4.2 Protocolo 1

Este protocolo considera o uso de uma terceira entidade confiável, denominada **Juiz**. Esta entidade é a responsável por gerar e gerenciar o par de chaves

assimétricas que protegerá os documentos eletrônicos pertencentes aos membros de um grupo.

A criação do par de chaves ocorre mediante uma requisição enviada ao Juiz pelo líder do grupo, contendo os parâmetros t e n necessários ao esquema de Shamir e à identificação dos membros do grupo. A chave pública (*TKu*) criada pelo Juiz é certificada digitalmente por uma Autoridade Certificadora e enviada ao líder do grupo solicitante. A chave privada (*TKr*) deste par é submetida ao esquema de compartilhamento de segredos de Shamir, o que resulta em n partes desta chave. As partes resultantes são entregues aos membros do grupo cuja identificação consta na requisição enviada ao Juiz.

A autenticação entre membros do grupo e Juiz é realizada através de certificados digitais, portanto a identificação de cada membro constante na requisição entregue ao Juiz é composta pelo número serial do seu certificado e o nome da Autoridade Certificadora que o emitiu. A combinação destes dois atributos identificam de maneira única um certificado digital e por conseqüência o seu proprietário [HOU 01].

A fim de impedir que um agente malicioso obtenha chaves *TKr* mantidas sob a guarda do Juiz, estas chaves são destruídas tão logo elas sejam quebradas pelo algoritmo de compartilhamento de segredos, assim como também são destruídas as partes da chave *TKr* já entregues aos seus devidos destinatários.

São estabelecidos três requisitos de segurança que devem ser atendidos pelo Juiz, são eles:

1. Ser confiável;
2. Não publicar qualquer chave *TKr*, em momento algum;
3. Entregar partes TKr_i somente aos membros autorizados do grupo.

A criação de um par de chaves neste protocolo é realizada através dos seguintes passos:

1. O líder de um grupo envia ao Juiz uma requisição contendo:
    - O parâmetros t e n determinados pelo grupo;

- A identificação de todos os membros do grupo responsáveis pela confidencialidade dos documentos eletrônicos;
- O valor de *T*, o que representa o período de tempo em que o Juiz deve manter as partes da chave *TKr*.

2. O Juiz cria o par de chaves, *TKu* e *TKr*;
3. O Juiz calcula o resumo da chave *TKu*, utilizado na identificação segura deste par de chaves;
4. O Juiz envia a chave *TKu* e o seu resumo à *AC*;
5. A *AC* emite o certificado digital da chave *TKu* contendo no campo de extensão do certificado o resumo informado. Após a emissão a *AC* envia o certificado ao Juiz;
6. O Juiz envia o certificado ao emissor da requisição;
7. O Juiz quebra a chave *TKr* em n partes utilizando o esquema de Shamir configurado com os parâmetros t e n informados na requisição e executa o protocolo de construção de Stadler;
8. O Juiz destrói a chave *TKr*;
9. O Juiz assina digitalmente as partes TKr_i a fim de garantir-lhes autenticidade;
10. O Juiz armazena de forma segura as n partes, vinculadas ao resumo da chave *TKu* e às identificações dos membros informadas na requisição.

De posse da chave *TKu*, os membros do grupo podem utilizá-la para cifrar seus documentos, os quais têm sua confidencialidade assegurada durante o tempo *T*, ou enquanto os membros não reunirem-se em um número que os permita reconstruir a chave *TKr*. O tempo *T* é convencionado pelos próprios membros do grupo no momento em que o líder envia a requisição solicitando ao Juiz a emissão das chaves *TKu* e *TKr*.

A entrega das partes da chave *TKr* aos membros de um grupo é realizada através dos seguintes passos:

1. M_i solicita ao Juiz uma parte da chave *TKr* informando ao Juiz o resumo da chave *TKu* que identifica o par de chaves em questão;

2. O Juiz autentica M_i através do seu certificado digital;

3. O Juiz envia a parte TKr_i a M_i;

4. O Juiz destrói a parte TKr_i;

5. M_i confere a assinatura do Juiz constante em TKr_i e em seguida executa protocolo de verificação de Stadler.

A figura 6.7 ilustra a construção do par de chaves e a entrega das partes da chave *TKr* deste par, geradas pelo Juiz.

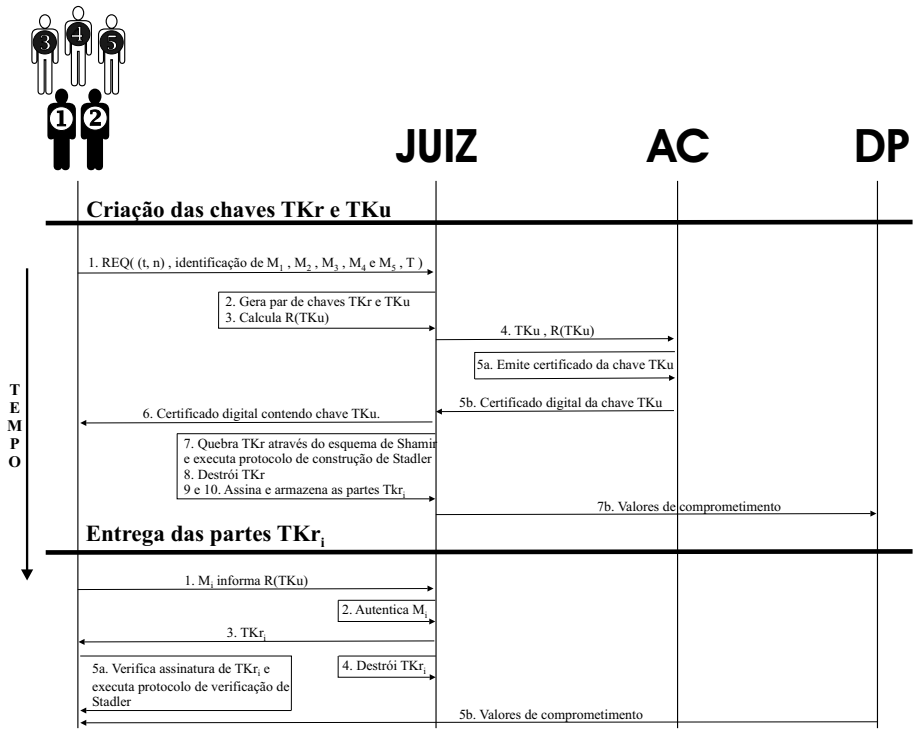

Figura 6.7: Protocolo 1: Os líderes do grupo são apresentados em destaque pelos membros identificados por 1 e 2. Os fluxos separados pelas linhas horizontais que percorrem a figura descrevem os passos necessários à criação do par de chaves *TKr* e *TKu* pelo Juiz, e a entrega das partes da chave *TKr* aos membros do grupo. A linha vertical representativa do tempo indica a seqüência em que os passos são executados.

Tendo a posse de uma das partes da chave *TKr*, M_i se torna responsável, junto com os demais membros que já possuem partes da chave *TKr*, a assegurar a confidencialidade dos documentos cifrados pela chave *TKu*.

Após expirado o tempo *T*, os membros do grupo executam o protocolo de reconstrução do esquema de Shamir para obter a chave *TKr* e então decifrarem os documentos cifrados com a chave *TKu*.

Caso não seja possível criar um subgrupo de entidades capaz de reconstruir a chave *TKr*, o protocolo deve ser encerrado e o grupo desfeito, já que esta situação traduz um cenário de membros hostis e que não possuem interesses iguais e tampouco são solidários uns com os outros.

6.4.3 Protocolo 2

Diferente de todos os protocolos apresentados até este momento, este protocolo caracteriza-se pela ausência de uma terceira entidade responsável pela criação e gerenciamento das chaves *TKr* e *TKu*. Estas funções são agora executadas individualmente por cada um dos membros do grupo que desejar tornar secreto o conteúdo de um documento durante um período de tempo *T*.

Em síntese, o funcionamento do protocolo consiste em cada membro do grupo criar o seu próprio par de chaves *TKr* e *TKu*, então identificados por M_i*TKr* e M_i*TKu*, e utilizar a chave M_i*TKu* para cifrar o seu documento que será posteriormente enviado a outro membro do grupo. Antes do envio do documento, a chave M_i*TKr* deve ser compartilhada pelo próprio M_i entre os demais membros através do esquema de Shamir.

O compartilhamento da chave M_i*TKr* deve ser realizado para que o membro que recebe o documento de M_i tenha garantias de que ele será capaz de decifrar o documento recebido após transcorrido o período de tempo *T*, mesmo que neste momento M_i se negue a cooperar na decifragem. Neste caso, para que a decifragem ocorra, o membro que tem a posse do documento, o qual chamaremos de M_j, sendo $j = 1, ..., n$ e $j \neq i$, deve informar aos demais membros do grupo que o membro M_i se nega a cooperar na decifragem do documento que ele próprio emitiu. Os demais membros do grupo devem

então se unir em um subgrupo que os permita a reconstruir a chave $M_i TKr$ e então recuperar a chave através do protocolo de reconstrução do esquema de Shamir. Recuperada a chave ela é entregue à M_j que pode então prosseguir com a decifragem do documento em questão.

A fase inicial do protocolo consiste na construção do par de chaves $M_i TKr$ e $M_i TKu$, sendo $i = 1, ..., n$, e no compartilhamento da chave $M_i TKr$. Esta fase é realizada através dos seguintes passos:

1. Os membros do grupo convencionam os valores dos parâmetros T e t;
2. O membro M_i cria um par de chaves $M_i TKr$ e $M_i TKu$;
3. M_i quebra a chave $M_i TKr$ em n partes utilizando o esquema de Shamir configurado com os parâmetros t e n, onde o valor de n é o total de membros do grupo menos um, já que é desnecessário que M_i gere uma parte da chave $M_i TKr$ para ele mesmo;
4. M_i assina digitalmente as partes $M_i TKr_j$ a fim de garantir-lhes autenticidade;
5. M_i executa o protocolo de construção de Stadler;
6. M_i envia cada $M_i TKr_j$ para M_j, sendo $j = 1, \ldots, n$ e $j \neq i$;
7. M_j executa o protocolo de verificação de Stadler.

A figura 6.8 ilustra o funcionamento desta fase inicial do protocolo.

Quando chega o momento da decifragem dos documentos, a fase final do protocolo, cada um dos membros têm a opção de entregar espontaneamente a sua chave $M_i TKr$ ao membro que recebeu o documento cifrado por $M_i TKu$. Este procedimento visa sobretudo diminuir esforço computacional e pessoal necessário à decifragem de um documento. Caso algum dos membros se negue a entregar a chave $M_i TKr$, os demais membros do grupo unem-se em um subgrupo de t entidades e podem reconstruir a chave $M_i TKr$ com base nas partes desta chave distribuídas por M_i no passo 6 da fase inicial do protocolo.

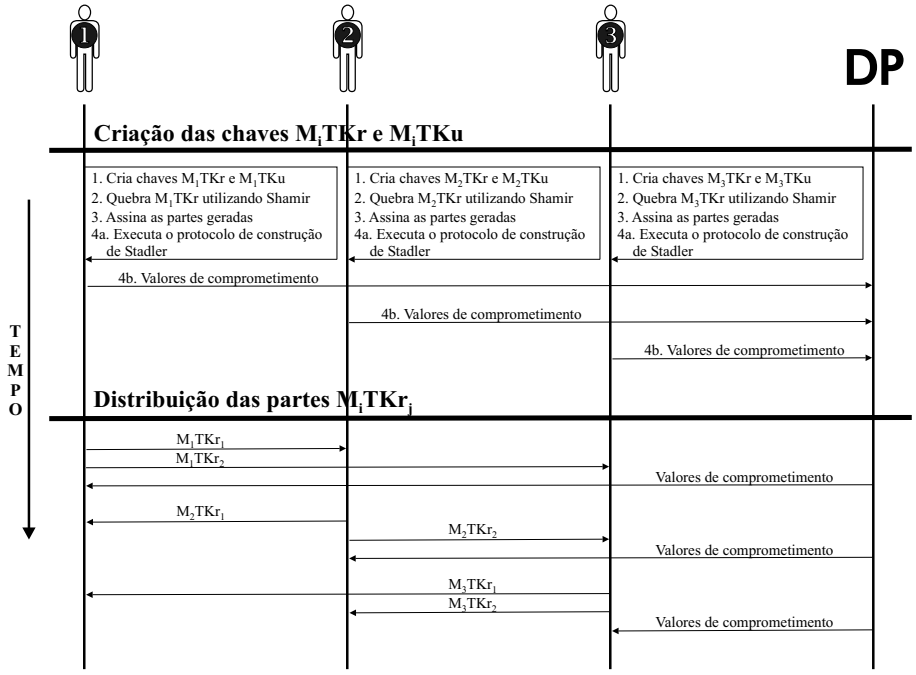

Figura 6.8: Protocolo 2: Cada membro do grupo executa individualmente os passos necessários à construção do par de chaves M_iTKr e M_iTKu, e à quebra da chave M_iTKr. Posteriormente cada membro compartilha as partes da sua chave M_iTKr entre os demais membros do grupo. A linha vertical representativa do tempo indica a seqüência em que os passos são executados.

Caso não seja possível criar um subgrupo de entidades capaz de reconstruir uma ou mais chaves *TKr*, o protocolo deve ser encerrado e o grupo desfeito, já que esta situação traduz um cenário de membros hostis e que não possuem interesses iguais e tampouco são solidários uns com os outros.

6.4.4 Protocolo 3

Este protocolo foi desenvolvido com base em *esquemas de compartilhamento de segredos sem o auxílio de uma entidade confiável* propostos em [ING 91, PED 91, JAC 95, STI 99] e descritos na seção 3.6, página 43 deste trabalho.

Tais esquemas permitem a construção cooperativa de um par de chaves *TKr* e *TKu*, sem que para isso seja necessário haver o conhecimento prévio da chave *TKr* por uma ou mais entidades. Através destes protocolos é possível criar primeiramente a

chave *TKu*, utilizá-la na cifragem de documentos eletrônicos e somente criar a chave *TKr* após transcorrido o tempo *T* convencionado previamente entre os membros do grupo.

Este protocolo prevê a construção compartilhada das chaves *TKu* e *TKr* pelos membros do grupo. Os esquemas que podem ser adotados neste protocolo são propostos por Torben Pryds Pedersen em [PED 91], que apresenta um esquema para a criação compartilhada de um par de chaves aplicáveis ao criptossistema assimétrico ElGamal, e por Dan Boneh e Matthew Franklin em [BON 01], cuja proposta consiste em um esquema para a construção compartilhada de um par de chaves aplicáveis ao criptossistema assimétrico RSA.

O funcionamento deste protocolo consiste na constituição inicial de um grupo de entidades, que convencionam o valor do período de tempo *T*. Em seguida, os membros do grupo constroem a chave *TKu* através de um dos esquemas citados no parágrafo anterior. Possuindo a chave *TKu*, os membros do grupo a utilizam para tornar secretos seus documentos. Neste momento, cada um dos membros que contribuíram para a construção da chave *TKu*, pode, junto com outros $t-1$ membros construir a respectiva chave *TKr*. Entretanto, considerando que todos têm interesse em manter seus próprios documentos confidenciais, eles devem respeitar o período de tempo *T* estabelecido por todos inicialmente.

Somente é possível comprometer a segurança do protocolo se um mínimo de t membros conspirarem entre si, conseguindo assim reconstruir a chave *TKr* antes do término do tempo *T*.

Após transcorrido o período de tempo *T*, os membros do grupo se reúnem, em um subgrupo com no mínimo t membros, e constroem a chave *TKr* através da união dos valores secretos mantidos por cada um destes membros.

Este protocolo destaca-se pela segurança proporcionada à chave *TKr*, pois considerando o fato que ela ainda não foi construída, não existe um local único que um agente malicioso possa tentar violar a fim de comprometer a chave *TKr*. Um agente malicioso somente obtém sucesso no comprometimento da chave *TKr* se ele comprometer a segurança de t valores secretos mantidos por t membros diferentes do grupo.

6.4.5 Protocolo com Anonimato

O envio anônimo de mensagens é requisito indispensável às aplicações que exigem a preservação da identidade de seus usuários. Exemplo destas aplicações é o processo de Licitação Pública, onde a identidade do licitante deve ser preservada até a sessão pública de abertura das propostas. Dentre os protocolos de criptografia temporal propostos neste capítulo, nenhum prevê o envio anônimo de mensagens, sendo portanto, inadequados para utilização em tais aplicações.

Visando suprir a carência deste requisito, é proposto nesta seção um protocolo baseado no uso de uma Rede de Misturadores responsável pela intermediação na comunicação entre os membros do grupo, mantendo desta forma anônimos os membros que enviarem mensagens a outros membros.

A Rede de Misturadores utilizada neste protocolo é constituída por um misturador principal, denotado *MIX*, e n misturadores secundários, denotados MIX_i sendo $i = 1, ..., n$. Cada um destes n misturadores secundários é responsável pelo encaminhamento das mensagens destinadas a um membro específico do grupo. Já as funções do misturador principal são criar os n misturadores secundários com base no parâmetro n que deve ser informado pelos membros do grupo, e posteriormente receber uma mensagem do membro que envia, e encaminhá-la ao misturador secundário responsável pelo envio de mensagens ao membro a quem se destina a mensagem em questão. As autenticações entre membro e misturador principal e entre membro e misturador secundário são realizadas através de certificados digitais.

Este protocolo utiliza o mesmo conceito de criação individual das chaves *TKr* e *TKu*, aplicado no protocolo apresentado na seção 6.4.3. Portanto, cada membro deve, após criar as chaves *TKr* e *TKu*, compartilhar a chave *TKr* com os demais membros do grupo. Considerando que o envio destas partes é realizado de forma anônima, ao término do protocolo os membros do grupo possuirão diversas partes de chaves *TKr* e serão incapazes de reconstruírem as chaves *TKr* necessárias pois eles não conseguirão unir as partes de uma mesma chave já que estas não possuem identificação alguma.

A solução para esta situação é alcançada utilizando um número aleatório

R gerado individualmente por cada membro do grupo. Este número é responsável por identificar qualquer documento ou informação que se relacione a um determinado par de chaves *TKr* e *TKu*, devendo ser enviado junto com documentos ou informações destinados a outro membro do grupo. Desta maneira, é possível que os demais membros do grupo reúnam informações relacionadas a uma determinada chave *TKr*. A cada execução do protocolo, deve ser escolhido um novo valor para *R* para evitar a associação do valor de *R* utilizado anteriormente à identidade de um membro. O tamanho de *R* deve adequado a fim de evitar que diferentes participantes escolham o mesmo número durante uma mesma execução do protocolo.

A fase inicial do protocolo consiste na construção do par de chaves M_i*TKr* e M_i*TKu* e no compartilhamento da chave M_i*TKr*. Esta fase é realizada através dos seguintes passos:

1. Os membros do grupo informam ao *MIX*, por meio de uma requisição, o valor de n e a identificação dos membros do grupo;
2. O *MIX* cria os n misturadores secundários e relaciona cada um deles à identificação de um determinado membro do grupo;
3. Os membros do grupo convencionam os valores dos parâmetros *T* e t;
4. O membro M_i gera um par de chaves M_i*TKr* e M_i*TKu*;
5. M_i quebra a chave M_i*TKr* utilizando o esquema de Shamir configurado com os parâmetros t e n, onde o valor de n será o total de membros do grupo menos um;
6. M_i gera o número aleatório *R*;
7. M_i executa o protocolo de construção de Stadler. Na publicação dos valores de g, S e A_j's, exigidos pelo esquema de Stadler, estes valores devem ser relacionados a *R*, permitindo com isso que o membro que recebe uma parte da chave M_i*TKr* possa localizar no *DP* os valores necessários para a execução do protocolo de verificação;
8. M_i envia as partes da chave M_i*TKr*, destinadas aos membros M_j, sendo $j = 1, \ldots, n$ e $j \neq i$, ao *MIX*. Junto a cada parte é enviado o número *R*.

9. O *MIX* encaminha as partes da chave M_i*TKr* recebidas aos respectivos misturadores secundários relacionados aos destinatários de cada uma das partes;

10. O misturador *MIX*$_j$ encaminha a parte recebida para o membro M_j ($j = 1, \ldots, n$ e $j \neq i$);

11. M_j executa o protocolo de verificação de Stadler.

Ao término da fase inicial do protocolo, o membro M_i que criou e compartilhou a chave M_i*TKr* pode enviar documentos cifrados pela chave M_i*TKu* aos demais membros do grupo, mas sempre enviando junto a estes documentos o número identificador *R* e sempre realizando o envio através da Rede de Misturadores.

No momento da decifragem dos documentos, cada um dos membros têm a opção de entregar espontaneamente a sua chave M_i*TKr* ao membro que recebeu o documento cifrado por M_i*TKu*. Caso o membro M_i se negue a entregar a chave, os demais membros do grupo unem-se em um subgrupo de t entidades e reconstroem a chave M_i*TKr* com base nas suas partes distribuídas por M_i no passo 8 da fase inicial do protocolo.

6.5 Análise de Segurança

A análise de segurança dos protocolos de criptografia temporal em grupos visa mensurar a confiabilidade que eles oferecem. Esta confiabilidade refere-se ao grau de confidencialidade assegurado às chaves *TKr* necessárias à decifragem dos documentos eletrônicos envolvidos nos protocolos, e a garantia de divulgação destas chaves no tempo correto.

A garantia de não divulgação de chaves *TKr* antes do tempo *T*, bem como a garantia de divulgação destas após este tempo, oferecida pelos módulos MCH-1 e MCH-2 está diretamente relacionada à confiabilidade atribuída a eles. Através de processos de auditoria, é possível constatar a correta operação dos módulos e com isso adicionar garantia de confiabilidade a eles. O eventual comprometimento de uma chave *TKr* nestes módulos ou mesmo falhas nos seus funcionamentos, são evidenciados nos

registros internos mantidos por estes dispositivos, tornando fácil a sua constatação em processos de auditoria.

Já os protocolos baseados em esquemas de compartilhamento de segredos tem o seu grau de confiabilidade dependente do fato de cada cada membro do grupo ser ou não confiável, uma vez que eles são responsáveis conjuntamente pela não divulgação das chaves *TKr* envolvidas nos protocolos. Portanto, é interessante, de ordem prática, estabelecer a probabilidade de um membro ser ou não confiável, e conseqüentemente a probabilidade do protocolo ser ou não corrompido. Desta maneira, na tentativa de mensurar a segurança oferecida por estes protocolos, recorreu-se a modelos probabilísticos. A análise com base nestes modelos é apresentada no apêndice A.

6.6 Conclusão

Este capítulo apresentou um total de seis novos protocolos de criptografia temporal, propostos por este trabalho.

Mesmo tendo como principal objetivo a prestação de serviços de criptografia temporal em grupos de entidades, dois dos protocolos propostos podem ser utilizados de maneira individual, não sendo exigida a formação de um grupo. Estes protocolos são o MCH-1 e o MCH-2.

No protocolo MCH-1 é possível permitir que um subgrupo de líderes executem tarefas devidas a todos os líderes em conjunto. Para tanto, é necessário a adoção de esquemas de compartilhamento de segredos, algo ainda não atendido pelos procedimentos que compreendem este protocolo.

Os protocolos propostos neste capítulo terão sua aplicação prática analisada no capítulo subseqüente, onde eles serão responsáveis por manterem confidenciais propostas comerciais, envolvidas em um processo de licitação, durante um período de tempo previamente estabelecido, assegurando após expirado este período que todas as propostas envolvidas deixarão de ser confidenciais e poderão ser julgadas através de critérios que compõem o processo.

Capítulo 7

Protocolo Criptográfico para Envio de Propostas em Processos de Compras

7.1 Introdução

Neste capítulo é analisada a aplicação prática dos protocolos de criptografia temporal em grupos propostos no capítulo 6. A análise prática consiste na aplicação destes protocolos em processos de compra, mais especificamente em processos de licitação pública devido à ênfase dada a tais processos neste trabalho. Os protocolos de criptografia temporal são utilizados visando assegurar a confidencialidade das propostas comerciais entregues pelos fornecedores ao comprador em um processo de licitação, durante o período que antecede o evento oficial de julgamento de propostas.

A natureza dos processos de compra, em particular dos processos de licitação, contribuem para a aplicação prática dos protocolos de criptografia temporal propostos, pois estes processos caracterizam-se essencialmente pela interação entre um grupo de fornecedores com um comprador, onde os fornecedores enviam ao comprador suas propostas comerciais em envelopes lacrados que somente devem ser abertos em um momento futuro determinado previamente.

Considerando que os protocolos propostos no capítulo anterior são, em sua totalidade, aplicáveis a grupos de entidades, e também a natureza dos processos de

licitação, torna-se possível a utilização destes protocolos em tais processos. Entretanto, a utilização dos protocolos de criptografia temporal em grupos no envio de propostas em processos de licitação não é, por si só, suficiente para atender às necessidades inerentes a estes processos, tornando-se necessária a adoção de outros mecanismos que visem suprir as necessidades não atendidas pelos protocolos de criptografia temporal em grupos. Estes mecanismos são fornecidos por um protocolo criptográfico destinado a garantir a execução segura dos procedimentos que compreendem o envio de propostas comerciais em um processo de licitação.

Este capítulo destina-se à proposta deste protocolo e à adaptação dos protocolos de criptografia temporal em grupos ao contexto de um processo de licitação pública.

A seção 7.2 apresenta uma visão geral do protocolo para envio de propostas em processos de compra. Na seção 7.3 é apresentada a notação utilizada na descrição do protocolo. Na seção 7.4 é descrita a fase de configuração, a qual representa a fase inicial do protocolo. A seção 7.5 apresenta a fase de envio de propostas, na qual são realizados os procedimentos necessários ao envio de propostas para posterior avaliação do comprador. A seção 7.6 apresenta a fase de julgamento de propostas, a qual representa a última fase do protocolo e compreende os procedimentos necessários à abertura e julgamento das propostas, assim como os procedimentos necessários ao término do protocolo. Na seção 7.7 são apresentados os mecanismos de auditoria fornecidos pelo protocolo. Por fim, na seção 7.8 é analisado o atendimento dos requisitos de segurança de um processo de compra pelo protocolo de envio de propostas.

7.2 Visão Geral

O **protocolo criptográfico para envio de propostas em processos de compras** se propõe a viabilizar o envio seguro de propostas comerciais em processos de licitação pública realizados através da Internet, nas modalidades concorrência, tomada de preços e convite, assegurando a confidencialidade destas propostas durante o período de tempo que antecede o evento oficial de julgamento das mesmas, e também a demonstrar

a aplicabilidade prática dos protocolos de criptografia temporal propostos no capítulo 6.

O desenvolvimento deste protocolo foi realizado visando o atendimento aos requisitos de segurança estabelecidos na seção 1.1.1 deste trabalho, os quais retratam as necessidades inerentes a um processo de compra. Os requisitos são: *anonimato*, *verificabilidade*, *temporalidade*, *unicidade*, *confidencialidade*, *integridade*, *autonomia*, *irrefutabilidade (não-repúdio)*, *não coerção*, *legalidade (licitude)*, *auditoria interna*, *auditoria externa* e *disponibilidade*.

Este protocolo deve contemplar e garantir a segurança dos procedimentos que constituem o envio de propostas em um processo de licitação. Para tanto, é necessário que o protocolo ampare procedimentos básicos necessários à garantia dos requisitos de segurança citados no parágrafo anterior. Estes procedimentos são listados abaixo:

1. Elaboração e publicação do edital[1];
2. Envio pelos fornecedores ao comprador, de envelopes lacrados contendo suas propostas comerciais;
3. Envio pelo comprador aos fornecedores, de recibos que comprovem a entrega de suas propostas dentro das condições temporais exigidas pelo edital, nos casos em que os fornecedores tiverem este direito;
4. Abertura, na data prevista no edital, e análise do conteúdos dos envelopes entregues;
5. Julgamento das propostas habilitadas à disputa;
6. Homologação do fornecedor vencedor.

Cada um destes procedimentos desdobra-se em vários passos que devem ser realizados para que seja assegurada a segurança do processo como um todo. O protocolo para envio seguro de propostas descreve cada um destes passos no decorrer das três fases que o compõem: *fase de configuração*, *fase de submissão de propostas* e *fase*

[1]Edital: termo utilizado para referenciar o instrumento convocatório de um processo de licitação, embora este também pode referir-se a cartas convite utilizadas na modalidade de licitação convite. Este termo foi escolhido visando uma melhor compreensão do conteúdo deste capítulo.

de julgamento de propostas. Estas fases são descritas, respectivamente, nas seções 7.4, 7.5 e 7.6.

O uso dos protocolos de criptografia temporal em grupos neste protocolo tem por finalidades a garantia da confidencialidade das propostas de preço, entregues ao comprador, durante o período de tempo que antecede o evento oficial de julgamento das propostas, e a garantia de que neste evento oficial todas as propostas tidas sob a posse do comprador serão abertas, independente da vontade do fornecedor que a compôs.

Em processos de licitação, especificamente onde inexiste cadastro prévio de fornecedores e naqueles enquadrados nos tipos *de melhor técnica* ou *de técnica e preço*, exige-se o envio, ao comprador, de outros dois envelopes, além daquele que possui a proposta de preço de um fornecedor. Um destes é o *envelope de habilitação*, o qual contém documentos relativos à habilitação do fornecedor, o outro é o *envelope da proposta técnica*, o qual contém documentos técnicos exigidos pelo edital.

A descrição do protocolo para envio seguro de propostas considera somente o envio do envelope que contém a proposta de preço de um fornecedor, mas os mesmos mecanismos criados para construir e submeter este envelope ao comprador poderão ser estendidos para o envio dos outros dois tipos de envelopes.

Entretanto, atualmente, nem todos os documentos, passíveis de exigências em editais de licitação e que podem vir a integrar os envelopes de habilitação e proposta técnica, são emitidos em forma eletrônica, o que impede o uso deste protocolo no envio de tais envelopes. Uma das soluções para este problema é utilizar o serviço de *certificação digital de documentos* [AB 03], previsto para ser oferecido a partir do início do ano de 2003 por agências cartorárias brasileiras. Este serviço consiste na digitalização de documentos em meio papel e na assinatura digital do cartorário sobre o documento eletrônico resultante, o qual declara através deste ato que o documento eletrônico assinado é cópia fiel do seu original em meio papel. Desta maneira é concedido a um documento eletrônico fé pública e com base nisso ele deve ser aceito da mesma maneira que o seu original em meio papel. Outra solução para o problema é a emissão eletrônica de todos os documentos passíveis de exigência em um edital.

A condução de um processo de licitação é, normalmente, realizada por

uma **comissão de licitação**, cuja função é representar o comprador que promove o processo, onde seus membros são responsáveis conjuntamente pelos atos e procedimentos realizados durante o processo de licitação. Considerando este fato, o desenvolvimento do protocolo para envio seguro de propostas é realizado visando a interação entre fornecedores e a comissão de licitação, também havendo a interação destes com terceiras entidades.

As terceiras entidades utilizadas no protocolo são responsáveis pela prestação de serviços específicos, tais como certificação digital, datação de documentos eletrônicos e publicação de informações relativas ao protocolo.

A confidencialidade e autenticidade das informações envolvidas no protocolo são asseguradas pela utilização de certificados digitais. O serviço de certificação digital é prestado por uma Autoridade Certificadora.

A correta localização temporal de todos os documentos envolvidos em um processo de licitação é fundamental para assegurar a validade deste, podendo ser decisivo em eventuais disputas envolvendo questões relacionadas ao atendimento ou não de prazos estabelecidos no edital regulamentador do processo. A autenticação temporal dos documentos envolvidos no protocolo é realizada por uma Autoridade de Datação.

A natureza pública dos processos de licitação exige a utilização de uma entidade responsável pela publicação das informações relativas ao processo de licitação e por conseqüência ao protocolo de envio seguro de propostas. A entidade utilizada para este fim é um diretório público, estruturado com base em recomendações criadas por órgãos técnicos competentes, como por exemplo as recomendações ITU-T X.500 e LDAP.

As seções seguintes descrevem a notação utilizada na descrição do protocolo de envio seguro de propostas e as fases que o compõem.

7.3 Notação

T : período de tempo em que o as propostas de preço enviadas ao comprador devem permanecer secretas;

h : índice identificador, sendo $h = 1, ..., n_C$;

i : índice identificador, sendo $i = 1, ..., n_F$;

$\boldsymbol{C}_h$: membro da comissão;

$\boldsymbol{F}_i$: fornecedor;

$\boldsymbol{P}_i$: proposta comercial enviada ao comprador por F_i;

TKr : chave privada que deve ser mantida secreta durante o período de tempo *T*;

TKu : chave pública correspondente a *TKr*;

$\boldsymbol{TKr}_C$: parte da chave *TKr* gerada pelo esquema de divisão do segredo e compartilhada entre os membros da comissão de licitação;

$\boldsymbol{TKr}_F$: parte da chave *TKr* gerada pelo esquema de divisão do segredo e compartilhada entre os fornecedores participantes da licitação;

$\boldsymbol{TKr}_{C_h}$: parte de TKr_C gerada através do esquema de Shamir, identificada pelo índice h;

$\boldsymbol{TKr}_{F_i}$: parte de TKr_F gerada através do esquema de Shamir, identificada pelo índice i;

t_C : limiar do esquema de Shamir utilizado no esquema de compartilhamento da parte TKr_C;

t_F : limiar do esquema de Shamir utilizado no esquema de compartilhamento da parte TKr_F;

n_C : número total de membros da comissão de licitação;

n_F : número total de fornecedores;

k_i : número aleatório gerado por F_i;

R(D) : resumo de um documento *D*;

S(D) : assinatura realizada em um documento *D*;

$\boldsymbol{P_i^{TKu}}$: P_i cifrada com a chave *TKu*;

REC : um recibo;

AC : Autoridade Certificadora;

AD : Autoridade de Datação;

DP : Diretório Público.

7.4 Fase de Configuração

Esta é a fase inicial do protocolo onde são obtidos os elementos básicos necessários às demais fases.

Nesta fase ocorre a elaboração e publicação do edital, a formação do grupo de pessoas que atuará no protocolo, a obtenção de uma ou mais chaves *TKu* através da execução do protocolo de criptografia temporal adotado e o protocolo do início do período de entrega de propostas.

A elaboração do edital ocorre através de um processo administrativo, o qual não é amparado por este protocolo, realizado pela comissão de licitação responsável. Após a elaboração do edital ele é tornado público pela comissão através do diretório público (*DP*), onde todos os possíveis interessados em concorrer no processo poderão conhecer seus detalhes através da obtenção deste edital.

A formação do grupo ocorre após a publicação do edital, através de uma etapa de comprometimento. Este comprometimento consiste no envio à comissão de licitação, pelo fornecedor interessado, de um termo assinado digitalmente onde declara a concordância com as condições estabelecidas no edital e seu interesse em participar do processo de licitação. Dentre as condições estabelecidas no edital, está a que determina o valor de *T*, que representa o período de tempo em que as propostas deverão permanecer secretas. O período de tempo *T* equivale ao intervalo de tempo compreendido entre as datas de início e término do **período de entrega de propostas**, estabelecidas no edital. O período de entrega de propostas refere-se ao espaço de tempo em que deve ocor-

rer a entrega das propostas. Propostas entregues fora deste período tornam-se inaptas à participação no processo.

Estruturalmente o grupo é formado pelos membros da comissão de licitação C_h, sendo $h = 1, ..., n_C$, e pelos fornecedores que participam do processo, F_i, sendo $i = 1, ..., n_F$. Os líderes do grupo são os membros da comissão de licitação.

A necessidade de formação do grupo é conseqüência da utilização dos protocolos de criptografia temporal em grupos, assim como a necessidade de designação de líderes para o grupo.

Após formado o grupo, deve ser executado o protocolo de criptografia temporal a fim de obter uma ou mais chaves *TKu* que serão utilizadas na cifragem das propostas. A quantidade de chaves *TKu* a serem criadas depende do protocolo utilizado. Os protocolos de criptografia temporal propostos no capítulo 6 foram adaptados ao contexto de processos de licitação e são assim descritos nas seções 7.4.1 e 7.4.2.

Após a execução do protocolo de criptografia temporal e na data prevista no edital a comissão de licitação oficializa o início do período de entrega de propostas através de um protocolo junto à *AD*. O recibo emitido pela *AD* deve ser publicado pela comissão no *DP* e servirá como marco inicial deste período. A data constante neste recibo também marca o início do período de tempo *T*.

Formalmente, esta etapa do protocolo é constituída pelos passos descritos abaixo:

1. A comissão elabora o edital;
2. A comissão publica o edital através do *DP*;
3. A comissão promove a formação do grupo que participará do protocolo;
4. O grupo formado executa o protocolo de criptografia temporal adotado no processo;
5. A comissão protocola o início do período de entrega de propostas;
6. A comissão publica o recibo obtido com o protocolo.

7.4.1 Utilização dos Protocolos Baseados em Módulos Criptográficos de Hardware

Os protocolos de criptografia temporal baseados em módulos criptográficos de hardware não sofrem qualquer alteração nos seus procedimentos durante a sua adaptação ao contexto de processos de licitação.

As seções 7.4.1.1 e 7.4.1.1 descrevem os protocolos MCH-1 e MCH-2 sendo utilizados em um processo de licitação.

7.4.1.1 Utilização do Protocolo MCH-1

Em um processo de licitação, as chaves *TKr* e *TKu* criadas pelo módulo MCH-1 são utilizadas na cifragem e decifragem, respectivamente, das propostas entregues à comissão de licitação.

A requisição enviada ao módulo e necessária à criação do par de chaves *TKr* e *TKu* deve ser emitida pelos membros da comissão de licitação. Nesta requisição os membros da comissão devem informar a data de divulgação da chave *TKr*, o que corresponde à data em que ocorrerá o evento oficial de julgamento de propostas, e o código secreto de cada um dos membros da comissão de licitação, cifrados pela chave pública do MCH-1.

Em resposta ao recebimento desta requisição o MCH-1 procede com a criação do par de chaves através dos passos descritos no protocolo original (seção 6.3.2, página 78) e com o envio do certificado digital contendo a chave *TKu* aos membros da comissão.

Após obter o certificado digital, a comissão de licitação o divulga no *DP* para que todos os demais membros do grupo utilizem esta chave na cifragem de suas propostas.

7.4.1.2 Utilização do Protocolo MCH-2

A utilização deste protocolo também fornece um único par de chaves *TKr* e *TKu* para ser utilizado na cifragem e decifragem das propostas.

Considerando o funcionamento do MCH-2, descrito na seção 6.3.2, a sua utilização em um processo de licitação não requer qualquer interação direta com o módulo, apenas com o diretório público através do qual ele torna públicas as chaves *TKr* e *TKu*.

A utilização do MCH-2 no processo de licitação consiste em os membros da comissão de licitação selecionarem, no diretório público utilizado pelo MCH-2, uma chave *TKu* que terá a sua respectiva chave *TKr* divulgada na data em que ocorre o evento oficial de julgamento de propostas.

Após selecionado o certificado digital que contém a chave *TKu*, os membros da comissão de licitação o divulga no *DP* para que todos os demais membros do grupo utilizem esta chave na cifragem de suas propostas.

7.4.2 Utilização dos Protocolos Baseados em Compartilhamento de Segredos

Os protocolos baseados em compartilhamento de segredos sofrem algumas alterações para a adaptação ao contexto de processos de licitação. Tais alterações se fizeram necessárias para que seja assegurada a presença dos membros da comissão de licitação na abertura das propostas. Desta maneira, nenhuma proposta pode ser aberta sem a presença de um determinado número de membros da comissão de licitação.

As alterações consistem no acréscimo do esquema de *divisão do segredo* no compartilhamento de chaves *TKr* e na adequação do esquema de verificabilidade ao esquema de divisão do segredo.

Neste novo modelo o compartilhamento de uma chave *TKr* deve ser inicialmente realizado através do esquema de divisão do segredo, o qual gera duas partes, TKr_C e TKr_F, a partir da chave *TKr*. Estas duas partes são submetidas ao esquema de Shamir tendo como respectivos parâmetros (n_C, t_C) e (n_F, t_F).

As figuras 7.1 e 7.2 apresentam respectivamente os protocolos de construção e reconstrução contidos no esquema de Divisão do Segredo e que são utilizados, respectivamente, para quebrar e reconstruir a chave *TKr*.

Esquema de Divisão do Segredo: Protocolo de Construção

1. Escolhe-se um número primo *p* de maneira aleatória, respeitando a condição que exige que *p* seja maior que *TKr*;

1. Escolhe-se um número randômico pertencente a Z_p, TKr_C;

3. Calcula-se o valor de TKr_F:

$$TKr_F = TKr - TKr_C \pmod p$$

Obs.: O número p será também utilizado no esquema de Shamir, no compartilhamento das partes TKr_C *e* TKr_F.

Figura 7.1: Esquema de Divisão do Segredo - Protocolo de Construção: Neste protocolo são obtidas as partes TKr_C e TKr_F, a partir da chave *TKr*. Estas partes serão posteriormente submetidas ao esquema de Shamir para a geração das partes que serão entregues aos membros do grupo.

Esquema de Divisão do Segredo: Protocolo de Reconstrução

1. t_1 membros da comissão e t_2 fornecedores devem cooperar a fim de obterem os valores de TKr_C e TKr_F, utilizando para isso o protocolo de reconstrução de Shamir;

2. Obtidos os valores de TKr_C e TKr_F, o valor de *TKr* é encontrado através da equação:

$$TKr = TKr_C + TKr_F \pmod p$$

Figura 7.2: Esquema de Divisão do Segredo - Protocolo de Reconstrução: Neste protocolo ocorre a reconstrução da chave *TKr* através das suas partes TKr_C e TKr_F.

As partes geradas com a quebra da parte TKr_C, denotadas por TKr_{C_h}, sendo $h = 1, ..., n_C$, são distribuídas entre os membros da comissão de licitação, enquanto as partes geradas a partir de TKr_F, denotadas por TKr_{F_i}, sendo $i = 1, ..., n_F$, são distribuídas entre os fornecedores.

Uma chave *TKr* compartilhada através deste modelo somente pode ser reconstruída a partir da união das partes TKr_C e TKr_F, o que por sua vez exige a cooperação de t_C membros da comissão de licitação e t_F fornecedores membros do grupo.

O modelo de verificabilidade utilizado nestes protocolos é composto por dois esquemas, ambos descritos em [STA 96], os quais são individualmente utilizados

para a verificabilidade das partes obtidas com o esquema de divisão do segredo e das partes obtidas com o esquema de Shamir. As figuras 7.3 e 7.4 apresentam respectivamente os protocolos de construção e verificação do esquema de verificabilidade que compõem este modelo.

Esquema de Verificabilidade: Protocolo de Construção

1. Quebra-se a chave *TKr* utilizando o protocolo de construção do esquema de divisão do segredo;
2. Escolhe-se um número gerador *g* pertencente ao conjunto Z_p^* (conjunto gerado através do número primo *p* utilizado nos esquemas de divisão do segredo e de Shamir);
3. Utilizando a chave *TKr* e as suas partes TKr_C e TKr_F geradas no passo 1, calcula-se os seguintes valores:
$$S = g^{TKr} \ , \ S_C = g^{TKr_C} \quad e \quad S_F = g^{TKr_F}$$
4. Quebra-se as partes TKr_C e TKr_F utilizando o protocolo de construção do esquema de Shamir;
5. Utilizando os coeficientes do polinômio *f(x)* criado no passo 4 para quebrar a parte TKr_C, calcula-se os seguintes valores:
$$A_i = g^{a_i} \ (sendo\ i = 1, \ldots, t_C - 1)$$
6. Utilizando os coeficientes do polinômio *f(x)* criado no passo 4 para quebrar a parte TKr_F, calcula-se os seguintes valores:
$$A_j = g^{a_j} \ (sendo\ j = 1, \ldots, t_F - 1)$$
7. Publica-se no *DP* os valores g, S, S_C, S_F, A_i e A_j relacionados à um dado identificador da chave *TKr*.

Figura 7.3: Esquema de Verificabilidade - Protocolo de Construção: Neste protocolo são calculados e publicados os valores de comprometimento (g, S, S_C, S_F, A_i e A_j).

7.4.2.1 Utilização do Protocolo 1

A utilização deste protocolo em um processo de licitação refere-se à utilização dos serviços fornecidos pela entidade confiável denominada Juiz na criação das chaves *TKr* e *TKu* e no gerenciamento da distribuição das partes da chave *TKr* entre os membros do grupo atuante no protocolo.

A requisição enviada ao Juiz e necessária à criação das chaves *TKr* e *TKu* deve ser emitida pelos membros da comissão de licitação. Nesta requisição deve ser informada a identificação de todos os membros do grupo, devidamente enquadrados nas

Esquema de Verificabilidade: Protocolo de Verificação

1. Cada parte TKr_{C_h} é enviada ao membro da comissão C_h, sendo $h = 1, \ldots, n_C$ e cada parte TKr_{F_i} é enviada ao fornecedor F_i, sendo $i = 1, \ldots, n_F$.

2a. Cada membro C_h verifica a integridade da sua própria parte TKr_{C_h} através da equação:

$$S_{C_h} = S_C \cdot \prod_{I=1}^{t_C - 1} A_i^{x_h^i}$$

A parte TKr_{C_h} somente deve ser considerada correta se satisfizer a equação:

$$S_{C_h} = g^{TKr_{C_h}}$$

2b. Cada fornecedor F_i verifica a integridade da sua própria parte TKr_{F_i} através da equação:

$$S_{F_i} = S_F \cdot \prod_{j=1}^{t_F - 1} A_j^{x_i^j}$$

A parte TKr_{F_i} somente deve ser considerada correta se satisfizer a equação:

$$S_{F_i} = g^{TKr_{F_i}}$$

2c. Qualquer membro do grupo, fornecedor ou membro da comissão,pode constatar a integridade das partes TKr_C e TKr_F através da equação:

$$S = S_C \cdot S_F$$

3. Se o resultado for positivo C_h e F_i informam a todos através do envio de uma mensagem de aceitação, caso contrário enviam uma mensagem de rejeição, encerrando o protocolo em seguida.

Figura 7.4: Esquema de Verificabilidade - Protocolo de Verificação: Este protocolo permite ao destinatário de uma parte de TKr_C ou TKr_F constatar a integridade da parte recebida. Permite ainda que todos constatem a integridade das partes TKr_C ou TKr_F.

categorias de fornecedores ou membros da comissão, os valores dos parâmetros (n_C, t_C) e (n_F, t_F), e o valor de *T*.

A criação das chaves *TKr* e *TKu* obedece os mesmos passos descritos no protocolo original (seção 6.4.2, página 87), exceto nos passos que descrevem o compartilhamento da chave *TKr* e a assinatura das partes geradas, pois o Juiz deve realizar o compartilhamento utilizando o esquema de divisão de segredo em conjunto com o esquema de Shamir. Em relação às assinaturas das partes, necessárias para garantir a autenticidade destas, somente as criadas pelo esquema de Shamir devem ser assinadas, pois as geradas pelo esquema de divisão do segredo não são entregues a nenhum dos membros do grupo.

Após a realização do compartilhamento da chave *TKr*, o Juiz destrói as partes TKr_C e TKr_F e armazena de forma segura as partes TKr_{C_h} e TKr_{F_i}, sendo

$h = 1, ..., n_C$ e $i = 1, ..., n_F$, vinculadas ao resumo da chave *TKu* e relacionadas às identificações dos membros do grupo informadas na requisição, respeitando o enquadramento de cada um destes.

A entrega das partes da chave *TKr* aos membros de um grupo é realizada através dos mesmos passos descritos no protocolo original, alterando somente o esquema de verificabilidade que deve ser realizado individualmente por cada membro visando a verificação da integridade das partes distribuídas pelo Juiz.

7.4.2.2 Utilização do Protocolo 2

O uso deste protocolo em um processo de licitação transfere aos fornecedores as responsabilidades de criação e gerenciamento das chaves *TKr* e *TKu*.

Cada fornecedor F_i deve criar um par de chaves F_i*TKr* e F_i*TKu* e utilizar a chave F_i*TKu* na cifragem da sua proposta. Já a chave F_i*TKr*, F_i deve compartilhá-la entre os demais fornecedores e membros da comissão de licitação através dos esquemas de divisão do segredo e de Shamir.

Os passos que compreendem a criação do par de chaves pelo fornecedor F_i e o compartilhamento da chave privada deste par entre os demais membros do grupo são iguais aos descritos no protocolo original (seção 6.4.3, página 91) com exceção aos esquemas de compartilhamento e verificabilidade que devem ser utilizados.

7.4.2.3 Utilização do Protocolo 3

O uso deste protocolo em um processo de compra não altera em nada os passos que descrevem o protocolo original, o qual prevê a construção compartilhada de um par de chaves *TKr* e *TKu* pelos membros do grupo que desejam tornar confidenciais seus documentos cifrando-os com a chave *TKu* criada.

No contexto de um processo de licitação, o funcionamento deste protocolo consiste inicialmente na construção, pelos membros do grupo, da chave *TKu* através de um dos esquemas de compartilhamento de segredos sem o auxílio de uma entidade confiável propostos em [PED 91] e [BON 01]. A chave *TKu* criada nesta fase inicial deve

ser utilizada pelos fornecedores na cifragem das suas propostas.

Neste momento a chave *TKr* permanece desconhecida de todos, pois ela somente deve ser construída na fase de julgamento de propostas.

7.4.2.4 Utilização do Protocolo com Anonimato

A utilização deste protocolo implica na mudança de todos os passos que compreendem a interação entre membros do grupo no protocolo de envio de proposta, uma vez que o mesmo não provê anonimato aos seus participantes.

A obtenção das chaves *TKr* e *TKu* através deste protocolo utiliza o mesmo conceito de criação individual das chaves aplicado no Protocolo 2. Portanto cada fornecedor F_i deve criar um par de chaves F_i*TKr* e F_i*TKu*, onde a chave F_i*TKu* é utilizada na cifragem da sua proposta e a chave F_i*TKr* deve ser compartilhada através dos esquema de divisão do segredo e de Shamir.

Tanto o compartilhamento da chave F_i*TKr* quanto a verificação de partes são realizadas através dos mesmos passos descritos no protocolo original (seção 6.4.5), alterando apenas os esquemas de compartilhamento e verificabilidade adotados.

7.5 Fase de Envio de Propostas

Esta fase do protocolo compreende os procedimentos necessários ao envio de propostas à comissão de licitação.

O funcionamento desta fase consiste em cada fornecedor F_i elaborar a sua proposta P_i. Após a elaboração das propostas, os fornecedores devem cifrá-las utilizando a chave *TKu*, obtida com a execução do protocolo de criptografia temporal. A cifragem das propostas visa torná-las confidenciais durante o período de tempo *T*. Às propostas cifradas, então identificadas por P_i^{TKu}, deverão ser anexados valores k_i, escolhidos pelos fornecedores de maneira aleatória. Estes valores serão posteriormente utilizados pela comissão de licitação na criação dos recibos REC_i que deverão ser enviados aos fornecedores confirmando o recebimento das propostas pela comissão e declarando as condições temporais em que estas foram entregues. O conjunto $P_i^{TKu}||k_i$ deverá então ser

assinado por F_i afim de conferir autenticidade ao conjunto. O conjunto assinado é identificado por $S_{F_i}(P_i^{TKu}||k_i)$. A assinatura sobre $P_i^{TKu}||k_i$ é requisito para que a proposta possa concorrer no processo de licitação, pois caso inexista não é possível provar a autoria de F_i.

Após a realização destes passos, o fornecedor F_i deve enviar $S_{F_i}(P_i^{TKu}||k_i)$ à comissão de licitação. Este envio deve ser precedido pela autenticação mútua entre fornecedor e membro da comissão. A autenticação deve ser realizada através de certificados digitais e visa tornar segura a identificação das partes comunicantes.

Formalmente, esta fase do protocolo é constituída pelos seguintes passos:

1. F_i elabora sua proposta P_i;
2. F_i cifra P_i utilizando a chave *TKu*, P_i^{TKu};
3. F_i gera de maneira aleatória um número k_i;
4. F_i anexa à proposta cifrada P_i^{TKu} o valor k_i, $P_i^{TKu}||k_i$;
5. F_i assina o conjunto $P_i^{TKu}||k_i$, $S_{F_i}(P_i^{TKu}||k_i)$;
6. F_i e um dos membros da comissão de licitação (C_h) autenticam-se mutuamente;
7. F_i envia $S_{F_i}(P_i^{TKu}||k_i)$ a C_h;
8. C_h recebe $S_{F_i}(P_i^{TKu}||k_i)$ e confere a assinatura de F_i;
9. C_h extrai k_i de $S_{F_i}(P_i^{TKu}||k_i)$;
10. C_h calcula o resumo de $S_{F_i}(P_i^{TKu}||k_i)$, $R(S_{F_i}(P_i^{TKu}||k_i))$;
11. C_h envia k_i e $R(S_{F_i}(P_i^{TKu}||k_i))$ à *AD* em requisições diferentes;
12. *AD* gera os recibos de protocolo $REC_{AD}(k_i)$ e $REC_{AD}(R(S_{F_i}(P_i^{TKu}||k_i)))$ e os envia à C_h;

13. C_h gera *REC*$_i$ assinando sobre o recibo gerado pela AD:

$$REC_i = S_{C_h}(REC_{AD}(k_i))$$

14. C_h envia *REC*$_i$ à F_i;

15. C_h armazena os valores k_i, *REC*$_i$, *REC*$_{AD}$*(R(S*$_{F_i}$*(P*$_i^{TKu}$*||k*$_i$*)))* e *S*$_{F_i}$*(P*$_i^{TKu}$*||k*$_i$*)* vinculados entre si;

16. C_h divulga no *DP* o valor de k_i.

A publicação dos valores k_i visa comprometer a comissão de licitação com a abertura das propostas respectivas àqueles valores, impedindo com isto que a comissão deixe de abrir uma ou mais propostas em benefício dos fornecedores que as compuseram.

A datação sobre *S*$_{F_i}$*(P*$_i^{TKu}$*||k*$_i$*)* visa estabelecer o tempo em que esta proposta foi entregue, impedindo com isto que o fornecedor utilize o mesmo número k_i para enviar outra proposta após a expiração do período de entrega de propostas.

Os procedimentos utilizados na criação do recibo foram estabelecidos objetivando não conceder ao fornecedor maneiras dele provar a outrém qual foi a sua proposta enviada à comissão, impedindo desta maneira que ele influencie os atos de outros participantes da licitação.

Durante o período de envio de propostas, um fornecedor pode enviar quantas propostas ele desejar. Porém, cada proposta enviada sobrepõe a sua anterior. Desta maneira, no julgamento das propostas é considerada somente a última proposta enviada pelo fornecedor. Isto se deve ao fato que cada fornecedor tem o direito de concorrer com uma única proposta.

7.6 Fase de Julgamento de Propostas

Esta fase representa o término do protocolo, aqui são divulgados os valores necessários à constatação da regularidade do protocolo. É encerrado o período de

entrega de propostas, são obtidas as chaves *TKr* necessárias à decifragem das propostas e ocorre o julgamento destas.

No momento inicial desta fase a comissão deve tornar pública uma relação contendo os valores descritos abaixo, relacionados com os valores k_i publicados na fase anterior:

- Os recibos REC_i;
- Os recibos $REC_{AD}(R(S_{F_i}(P_i^{TKu}||k_i)))$;
- As propostas cifradas e assinadas, $S_{F_i}(P_i^{TKu}||k_i)$.

Esta relação deve ser assinada pelos membros da comissão e protocolizada na *AD*. A publicação destes valores visa comprometer a comissão de licitação em relação às propostas que serão julgadas no processo e demonstrar a regularidade destas quanto ao atendimento aos requisitos temporais do edital.

Simultâneo a esta publicação, a comissão deve oficializar o término do período de entrega de propostas através de um protocolo junto à *AD*, encerrando assim este período e com isso o período *T*.

O passo seguinte consiste na obtenção de uma ou mais chaves *TKr* necessárias à abertura das propostas. Os passos a serem realizados para esta obtenção dependem do protocolo de criptografia temporal em grupos utilizado. Abaixo são descritos estes passos de acordo com cada um destes protocolos:

Protocolo MCH-1: A obtenção da chave *TKr* respectiva à chave *TKu* utilizada na cifragem das propostas ocorre através de uma solicitação feita ao módulo MCH-1 pelos membros da comissão, onde estes informam o resumo contido no certificado digital da chave *TKu* e os códigos secretos informados na requisição enviada ao módulo no momento da criação das chaves *TKr* e *TKu*.

O MCH-1 somente entrega a chave *TKr* aos membros da comissão se for constatado o atendimento dos requisitos de segurança de temporalidade e autenticação, conceituados na seção 6.3.2.

Se ambos os requisitos forem satisfeitos, o módulo envia aos membros da comissão de licitação a chave *TKr*.

Protocolo MCH-2: A obtenção de uma chave *TKr* através do módulo MCH-2 é mais simples e não exige interação entre o usuário do serviço e o módulo, apenas entre o usuário e o diretório público utilizado pelo MCH-2 para a publicação das chaves *TKr* e *TKu*. Portanto, os membros da comissão de licitação devem localizar e obter neste diretório público a chave *TKr* respectiva à chave *TKu* utilizada na cifragem das propostas. Entretanto, a comissão de licitação somente terá sucesso na localização e obtenção desta chave, caso já tenha transcorrido o período de tempo, estabelecido pelo módulo, em que esta chave deve permanecer oculta.

Protocolo 1: Neste protocolo as chaves *TKr* e *TKu* são criadas pelo Juiz e este compartilha a chave *TKr* aos participantes do processo de licitação durante o decorrer do período de envio de propostas. Portanto, a obtenção da chave *TKr* é realizada através da cooperação entre os membros componentes do grupo atuante na licitação.

Após expirado o tempo *T* um mínimo de t_C membros da comissão e um mínimo de t_F fornecedores executam o protocolo de reconstrução do esquema de Shamir e em seguida o protocolo de reconstrução do esquema de Divisão do Segredo, recuperando desta maneira a chave *TKr*.

Protocolo 2: Neste protocolo cada fornecedor F_i é responsável por criar seu próprio par de chaves F_i*TKr* e F_i*TKu* e por compartilhar a chave F_i*TKr* entre os membros do grupo. Portanto é necessário que a comissão de licitação obtenha todas as chaves F_i*TKr*, sendo $i = 1, ..., n_F$.

Primeiramente cada fornecedor têm a opção de entregar espontâneamente a sua chave F_i*TKr* à comissão de licitação. Caso algum dos fornecedores se negue a entregar a chave F_i*TKr*, os membros da comissão de licitação unem-se em um subgrupo de t_C membros juntamente com um subgrupo de t_F fornecedores e reconstroem a chave F_i*TKr* com base nas partes desta chave distribuídas por F_i.

Protocolo 3: Neste protocolo a chave *TKu* utilizada na cifragem das propostas é construída de maneira cooperativa por todos os membros do grupo.

Assim como a construção da chave *TKu*, a construção da chave *TKr* ainda desconhecida de todos, é formada de maneira cooperativa entre os membros do grupo atuante na licitação. A construção da chave *TKr* ocorre com a reunião dos membros do grupo em um subgrupo com no mínimo t membros, a construção da chave *TKr* é feita através da união dos valores secretos mantidos por cada um destes membros.

Neste protocolo, todos os valores secretos mantidos por cada membro possui a mesma importância no momento da construção de cada uma das chaves, não havendo distinção entre membros da comissão e fornecedores.

Protocolo com Anonimato: Utilizando o mesmo conceito de criação individual aplicado no Protocolo 2, cada fornecedor F_i é responsável por criar seu próprio par de chaves F_i*TKr* e F_i*TKu* e por compartilhar a chave F_i*TKr* entre os membros do grupo. Portanto é necessário que a comissão de licitação obtenha todas as chaves F_i*TKr*, sendo $i = 1, ..., n_F$.

Primeiramente cada fornecedor têm a opção de entregar espontâneamente a sua chave F_i*TKr* à comissão de licitação. Caso algum dos fornecedores se negue a entregar a chave F_i*TKr*, os membros da comissão de licitação unem-se em um subgrupo de t_C membros juntamente com um subgrupo de t_F fornecedores e reconstroem a chave F_i*TKr* com base nas partes desta chave distribuídas por F_i.

Após obter as chaves *TKr* necessárias, a comissão de licitação decifra todas as propostas $S_{F_i}(P_i^{TKu}||k_i)$ e as julga de acordo com as condições estabelecidas no edital. Em seguida a comissão informa a todos qual foi a proposta vencedora, através de uma publicação no *DP*.

Uma relação contendo as chaves *TKr* utilizadas deve ser publicada no *DP* a fim de possibilitar aos membros do grupo e a terceiros a constatação da legitimidade da escolha da proposta vencedora.

7.7 Auditoria

O processo de auditoria constitui-se no exame de operações realizadas visando constatar a regularidade destas. No contexto deste trabalho, um processo de auditoria visa atribuir confiabilidade a um protocolo ou mesmo apontar falhas ou possíveis fraudes ocorridas durante a sua execução.

O protocolo criptográfico para envio de propostas provê meios que permitem a realização desta tarefa, os quais constituem-se das informações tornadas públicas durante a execução do protocolo.

A auditoria no protocolo para envio de propostas tem como objetivos:

- Verificar o cumprimento do requisito *temporalidade*;
- Constatar o cumprimento do requisito *unicidade*;
- Atestar a integridade das propostas que concorreram no processo;
- Verificar a abertura de todas as propostas entregues à comissão;
- Constatar a legitimidade na escolha da proposta vencedora.

Todo o processo de licitação é regulado por prazos estabelecidos no edital. O não atendimento destes prazos incorre no impedimento de participação ou mesmo na anulação do processo. Através do confrontamento dos recibos de protocolo de início e término do período de entrega de propostas com as datas constantes nos recibos $REC_{AD}(R(S_{F_i}(P_i^{TKu}||k_i)))$ divulgados no *DP*, é possível verificar se o prazo de entrega de propostas foi ou não respeitado.

O descumprimento do prazo de entrega de propostas somente é possível através da violação da integridade da *AD*, alterando a ordem e o tempo em que esta protocolou um determinado documento. A constatação deste evento somente é possível através de uma auditoria na *AD*.

A constatação do cumprimento do requisito unicidade é obtida através da análise das assinaturas constantes nas propostas publicadas. Este requisito é atendido

se cada fornecedor F_i membro do grupo possuir a sua assinatura em uma única proposta publicada.

A abertura de todas as propostas pode ser verificada através da comparação entre os valores k_i publicados durante a fase de envio de propostas com a relação de valores publicados na fase de julgamento de propostas. A existência de valores k_i não relacionados aos recibos REC_i e $REC_{AD}(R(S_{F_i}(P_i^{TKu}||k_i)))$ e a proposta $S_{F_i}(P_i^{TKu}||k_i)$ é indicativo de irregularidade no processo.

A integridade e autoria das propostas podem ser verificadas através das assinaturas nelas constantes.

A divulgação de todas as propostas que participaram da fase de julgamento e das respectivas chaves *TKr* permitem a qualquer pessoa constatar a legitimidade de escolha da proposta vencedora através da decifragem e comparação entre elas.

7.8 Análise Relativa ao Atendimento dos Requisitos de Segurança

Como já dito anteriormente, o desenvolvimento do protocolo para envio de propostas em processos de compra foi realizado visando o atendimento aos requisitos de segurança estabelecidos na seção 1.1.1. Portanto é necessária uma análise referente ao atendimento destes requisitos por este protocolo. Esta análise é apresentada na tabela 7.1.

7.9 Conclusão

Este capítulo apresentou o último protocolo proposto por este trabalho, consistindo em um protocolo que visa viabilizar o envio via Internet seguro de propostas comerciais em processos de compra.

Espera-se que através dele seja possível desenvolver soluções que viabilizem a realização via Internet de todos os procedimentos necessários ao processo de licitação.

Seu desenvolvimento objetivou atender a todos os requisitos de segurança de processos de compra estabelecidos e demonstrar na prática a aplicação dos protocolos de criptografia temporal em grupos, também propostos por este trabalho. Entretanto, o atendimento a todos os objetivos não foi possível visto que o requisito de anonimato não foi atendido. Este requisito possibilita eliminar a correlação entre propostas e fornecedores e com isso eventuais favorecimentos dados pela comissão de licitação a uns fornecedores em detrimento de outros. Entretanto, são necessárias alterações nos passos que compõem este protocolo, bem como a adoção de outras entidades, tal como uma rede de misturadores.

Em relação a utilização dos protocolos de criptografia temporal propostos, em um deles surge uma desvantagem. O protocolo em questão é o protocolo MCH-2 e a desvantagem refere-se a inflexibilidade em relação à mudança de data no período de julgamento de propostas, uma vez que não há meios de mudar datas de divulgação de chaves *TKr* mantidas pelo módulo. Nos demais protocolos esta desvantagem não ocorre devido à necessidade de um determinado número de membros do grupo cooperar a fim de obter as chaves criptográficas necessárias à abertura das propostas.

Tabela 7.1: Análise comparativa do protocolo para envio de propostas em relação aos requisitos de segurança de processos de compra.

Requisito de Segurança	**Análise**
Anonimato	Não atende. Este requisito somente poderia ser atendido com a utilização do protocolo de criptografia temporal com anonimato e realizando mudanças nos procedimentos que se referem à interação entre partes no protocolo de envio de propostas.
Verificabilidade	Atende, pois cada fornecedor obtém um recibo assinado por um dos membros da comissão de licitação, onde consta a data em que foi realizada a entrega da sua proposta.
Temporalidade	Atende, pois somente as propostas protocoladas durante o período de entrega de propostas poderão concorrer no processo.
Unicidade	Atende, pois na etapa de julgamento das propostas, deve haver uma única proposta para cada fornecedor membro do grupo atuante na licitação. A unicidade é constatada através das assinaturas constantes nas propostas.
Confidencialidade	Atende desde que o protocolo de criptografia temporal em grupos utilizado não sofra ataques que culminem no comprometimento da sua segurança.
Integridade	Atende através das assinaturas constantes nas propostas. Qualquer alteração em um proposta implica na impossibilidade de verificação da assinatura do fornecedor que a compôs, deixando desta forma, evidente a violação praticada.
Autonomia	Atende, pois os protocolos de criptografia temporal asseguram a decifragem de um documento eletrônico, protegido pelo protocolo, independente da vontade da pessoa que o cifrou.
Irrefutabilidade (não-repúdio)	Atende, pois sendo possível validar a assinatura constante em uma proposta através da chave pública de um fornecedor membro do grupo, este não poderá negar a sua autoria.
Não coerção	Atende, pois o fornecedor não recebe meios que o permitam provar a outrém qual foi o valor da sua proposta. O recibo REC_i emitido pela comissão permite somente que o fornecedor prove a realização de uma proposta.
Legalidade (licitude)	Este requisito não foi analisado por ter cunho jurídico, não fazendo parte do escopo deste trabalho.
Auditoria Interna	Atende, pois os membros do grupo podem constatar a regularidade do processo através da análise dos valores publicados no *DP*.
Auditoria Externa	Atende, pois terceiros podem constatar a regularidade do processo através da análise dos valores publicados no *DP*.
Disponibilidade	Atende, pois todas as propostas julgadas e as correspondentes chaves *TKr* são divulgadas no *DP* permitindo que qualquer pessoa as analisem.

Capítulo 8

Considerações Finais

O objetivo geral deste trabalho foi atendido no capítulo 6, onde foram propostos seis novos protocolos de criptografia temporal. Estes protocolos visam, em especial, a prestação de serviços de criptografia temporal para grupos, permitindo a seus membros obter o controle sobre o período de tempo em que são mantidos confidenciais seus documentos, e assegurando que estes deixarão de ser confidenciais após expirado o período de tempo pré-estabelecido.

Os dois primeiros protocolos de criptografia temporal propostos prevêem a construção de mecanismos de hardware com propriedades específicas de criação e gerenciamento de chaves criptográficas. Estes protocolos beneficiam-se da segurança física e lógica, possíveis de serem implementadas nestes mecanismos.

Os quatro protocolos restantes utilizam o conceito de confiança distribuída, aplicado através de esquemas de compartilhamento de segredos. A aplicação deste conceito permite a transferência aos membros do grupo da responsabilidade sobre a manutenção da confidencialidade dos documentos durante o período estabelecido, tornando-os assim solidários uns com os outros em relação aos prejuízos ou benefícios que possam vir a ser causados a qualquer um deles.

O desenvolvimento destes novos protocolos de criptografia temporal possibilitou a criação de um protocolo criptográfico voltado para processos de compras, em particular processos de licitação pública. Este protocolo é destinado a garantir a

execução segura de procedimentos que compreendem o envio de propostas comerciais em um processo de licitação. A utilização deste protocolo permite que estes procedimentos sejam realizados de maneira segura através da Internet, sem que para isso seja necessário deixar de atender algum dos requisitos inerentes a processos de licitação pública. Este protocolo permite a aplicação prática dos protocolos de criptografia temporal propostos.

O estabelecimento dos requisitos de segurança inerentes a processos de licitação pública ocorreu através do estudo de trabalhos científicos, da análise criteriosa da legislação que ampara estes processos e através de entrevistas com pessoas de notória competência na área de licitações públicas. Estes requisitos foram essenciais para direcionar o desenvolvimento do protocolo de envio de propostas em processos de compras.

Ainda considerando o atendimento aos objetivos específicos do trabalho, foram apresentadas análises de segurança sobre os protocolos propostos, visando mensurar o grau de segurança oferecida por eles. As análises foram realizadas através de diferentes métodos entre os protocolos propostos, sendo eles:

Métodos probabilísticos: utilizado na análise de segurança dos protocolos de criptografia temporal baseados em compartilhamento de segredos, onde buscou-se inferir o grau de segurança oferecido por estes protocolos considerando a probabilidade de corrupção apresentada por cada membro do grupo atuante em um protocolo;

Método comparativo: utilizado na análise de segurança do protocolo para envio de propostas em processos de compra, onde foi analisado e justificado o atendimento ou não dos requisitos de segurança de processos de compra estabelecidos.

O desenvolvimento de um sistema permitiu demonstrar a viabilidade de implementação dos protocolos propostos. Este sistema limitou-se à implementação somente de alguns módulos dos protocolos propostos. Porém, mostrou-se suficiente para atender ao último objetivo específico deste trabalho.

No contexto deste trabalho, as seguintes contribuições podem ser identificadas:

- Proposta de seis novos protocolos de criptografia temporal, passíveis de aplicação

em várias situações, em especial nas previstas pelo projeto **Cartório Virtual** em desenvolvimento no LabSEC;

- Proposta de um protocolo criptográfico que viabiliza de forma segura o envio via Internet de propostas comerciais em processos de licitação pública, especificamente nas modalidades concorrência, tomada de preços e convite;
- Abordagem e utilização de protocolos de criptografia temporal em uma situação real, processos de licitação pública;
- Estabelecimento de requisitos de segurança necessários a protocolos criptográficos direcionados a processos de compra, em particular a processos de licitação pública;
- Análise de protocolos criptográficos baseados em esquemas de compartilhamento de segredos utilizando modelos probabilísticos.

8.1 Trabalhos Futuros

A continuidade deste trabalho é possível através da realização de novas pesquisas e da implementação dos protocolos propostos. Sugestões para estes trabalhos são listadas abaixo:

- Analisar o modelo de compartilhamento de segredos adotado nos protocolos de criptografia temporal para grupos, utilizando um modelo probabilístico que admita diferentes probabilidades de desonestidade entre os membros do grupo;
- Estudar e propor esquemas de compartilhamento de segredos que flexibilizem a formação do grupo, no sentido de permitir que membros entrem ou saiam do grupo durante a execução do protocolo, sem comprometer a segurança deste;
- Projetar e construir os módulos criptográficos de hardware MCH-1 e MCH-2;
- Desenvolver um sistema de compras seguro que reúna todos os protocolos propostos neste trabalho e proporcione ao usuário a flexibilidade de escolha quanto ao protocolo de criptografia temporal a ser utilizado;

- Propor um protocolo criptográfico capaz de assegurar que a proposta comercial cifrada entregue por um fornecedor em um processo de licitação pública, seja uma proposta válida;

- Analisar as exceções cabíveis a processos licitatórios, tais como: prorrogação de prazos, cancelamento do processo, paralisação do processo por ordem judicial. E, com base nesta análise, adequar o protocolo de envio de propostas ou criar novas soluções para atender a estas exceções;

- Propor alterações nas leis brasileiras que regulamentam as compras de entidades públicas, a fim de tornar possível o uso da tecnologia de Segurança da Informação aliada à Internet em todas as modalidades de licitação;

- Utilizar os protocolos de criptografia temporal, propostos neste trabalho, na implementação de serviços previstos no projeto Cartório Virtual/LabSEC.

Referências Bibliográficas

[AB 03] ANOREG-BR. **Brasileiros poderão ter qualquer documento certificado digitalmente e fazer quantas cópias digitais quiser**. Disponível em <http://www.anoregbr.org.br/new/index.php?action=servicos>. Acesso em 06 de Fevereiro de 2003.

[APA 02] APACHE. **Apache Web Server**. Disponível em <http://www.apache.org/>. Acesso em 26 de Agosto de 2002.

[BON 00] BONEH, D.; NAOR, M. Timed commitments. **Proceedings of Crypto 2000**, [S.l.], p.236–254, 2000.

[BON 01] BONEH, D.; FRANKLIN, M. Efficient generation of shared rsa keys. **Journal of the ACM (JACM)**, [S.l.], v.48, p.702–722, Julho, 2001.

[BUL 98] BULDAS, A.; LAUD, P. New linking schemes for digital time-stamping. **The 1st International Conference on Information Security and Cryptology**, [S.l.], p.3–14, Dezembro, 1998.

[CHA 81] CHAUM, D. L. Untraceable electronic mail, return addresses, and digital pseudonyms. **Communications of the ACM**, [S.l.], v.24, n.2, p.84–90, 1981.

[CIT 99] CITADINI, A. R. **Comentários e Jurisprudência sobre a Lei de Licita cões Públicas**. 3th. ed. Editora Max Limonad Ltda, 1999.

[CRE 99] CRESCENZO, G. D.; OSTROVSKY, R.; RAJAGOPALAN, S. Conditional oblivious transfer and timed-release encryption. **Advances in Cryptology - EUROCRYPT'99**, [S.l.], 1999.

[CUS 01] CUSTÓDIO, R. F. Análise crítica da icp-brasil - resposta a consulta pública. Novembro, 2001.

[Dec] BRASIL. Decreto n. 4.264, de 10 de junho de 2002.

[DIA 03] DIAS, J. S.; CUSTODIO, R. F.; DEMÉTRIO, D. B. Sincronização segura de relógio para documentos eletrônicos. **Simpósio Brasileiro de Redes de Computadores - SBRC 2003**, [S.l.], v.2, p.585–598, Maio, 2003.

[DIF 76] DIFFIE, W.; HELLMAN, M. E. New directions in cryptography. **IEEE International Symposium on Information Theory**, [S.l.], Junho, 1976.

[FOR 97] FORD, W.; BAUM, M. S. **Secure Electronic Commerce - Building the Infrastructure for Digital Signatures and Encryption**. Prentice-Hall, Inc, 1997.

[GEN 96] GENNARO, R. **Theory and Practice of Verifiable Secret Sharing**. Massachusetts Institute of Technology, Maio, 1996. Tese de Doutorado.

[HAR 98] HARKAVY, M.; TYGAR, J. D.; KIKUCHI, H. Electronic auctions with private bids. **Proceedings of the 3rd USENIX Workshop on Electronic Commerce**, [S.l.], p.61–74, Setembro, 1998.

[HAT 02] HAT, R. **Linux Red Hat**. Disponível em <http://www.redhat.com/>. Acesso em 01 de Dezembro de 2002.

[HOU 01] HOUSLEY, R.; POLK, T. **Planning for PKI - Best Practies Guide for Deploying Public Key Infrastructure**. John Wiley & Sons, Inc, 2001.

[ING 91] INGEMARSSON, I.; SIMMONS, G. J. A protocol to set up shared secret schemes without the assistance of a mutually trusted party. **Advances in Cryptology - EUROCRYPT'90**, [S.l.], p.266–282, 1991.

[JAC 95] JACKSON, W.-A.; MARTIN, K. M.; O'KEEFE, C. M. Efficient secret sharing without a mutually trusted authority. **Advances in Cryptology - EUROCRYPT'95**, [S.l.], p.183–193, 1995.

[JAK 98] JAKOBSSON, M.; M'RAIHI, D. Mix-based electronic payments. **Selected Areas in Cryptography**, [S.l.], p.157–173, 1998.

[JAK 02] JAKOBSSON, M.; JUELS, A.; RIVEST, R. L. **Making Mix Nets Robust For Electronic Voting By Randomized Partial Checking**. citeseer.nj.nec.com/jakobsson02making.html.

[KUD 98] KUDO, M. Secure electronic sealed-bid auction protocol with public key cryptography. **IEICE Trans. Fundamentals**, [S.l.], v.E81, p.20–27, Janeiro, 1998.

[KUD 99] KUDO, M.; MATHURIA, A. An extended logic for analyzing timed-release public-key protocols. **Information and Communication Security - Second International Conference (ICICS'99)**, [S.l.], p.183–198, Novembro, 1999.

[LIP 02] LIPMAA, H.; ASOKAN, N.; NIEMI, V. Secure vickrey auctions without threshold trust. **Financial Cryptography 2002, Lecture Notes in Computer Science**, [S.l.], 2002.

[MAO 00] MAO, W. Sending message into a definite future: Non-parallelisable case. <**http://www.hpl.hp.com/techreports/2000/HPL-2000-86.pdf**>, [S.l.], Julho, 2000.

[MAO 01] MAO, W. Timed-release cryptography. <**http://www.hpl.hp.com/techreports/2001/HPL-2001-37.pdf**>, [S.l.], Março, 2001.

[MAY 93] MAY, T. C. **Timed-Release Crypto**. Disponível em <http://cypherpunks.venona.com/date/1993/02/msg00129.html>. Acesso em 04 de Setembro de 2002.

[MEI 90] MEIRELLES, H. L. **Direito Administrativo Brasileiro**. Editora Revista dos Tribunais, 1990.

[MEN 96] MENEZES, A. J.; VAN OORSCHOT, P. C.; VANSTONE, S. A. **Handbook of Applied Cryptography**. CRC Press, Outubro, 1996.

[MEY 83] MEYER, P. L. **Probabilidade - Aplicações à Estatística**. 2. ed. Livros Técnicos e Científicos Editora S.A., 1983.

[MIC 98] MICHAELIS, D. **Michaelis: moderno dicionário da língua portuguesa**. Standard. ed. Cia. Melhoramentos de São Paulo, 1998.

[MIC 02a] MICROSOFT, C. **CAPICOM**. Disponível em <http://msdn.microsoft.com/library/en-us/security/Security/capicom_reference.asp>. Acesso em 26 de Agosto de 2002.

[MIC 02b] MICROSOFT, C. **E-commerce no mundo do aço**. Disponível em <http://www.microsoft.com/brasil/casos/caso_usiminas.asp>. Acesso em 15 de Agosto de 2002.

[MIC 02c] MICROSOFT, C. **Java Script**. Disponível em <http://msdn.microsoft.com/scripting/jscript>. Acesso em 26 de Agosto de 2002.

[MIC 02d] MICROSOFT, C. **Microsoft Internet Explorer**. Disponível em <http://www.microsoft.com/windows/ie/default.asp>. Acesso em 26 de Agosto de 2002.

[MIC 02e] MICROSOFT, C. **VBScript**. Disponível em <http://msdn.microsoft.com/scripting/vbscript/>. Acesso em 26 de Agosto de 2002.

[MIC 02f] MICROSOFT, C. **Windows 2000**. Disponível em <http://www.windows.com>. Acesso em 01 de fevereiro de 2003.

[MYS 02] MYSQL. **MySQL Data Base**. Disponível em <http://www.mysql.com/>. Acesso em 26 de Agosto de 2002.

[NA 01] NETWORK ASSOCIATES, I.; COMPANIES, A. **PGP version 7.0.3 - User Guide**. Disponível em <ftp://ftp.pgpi.org/pub/pgp/7.0/docs/english/PGPWinUsersGuide.pdf>.

[NIE 00] NIEBUHR, J. M. **Princípio da Isonomia na Licita cão Pública**. Livraria e Editora Obra Jurídica Ltda, 2000.

[NIS 93a] NIST. Data encryption standard (des) - fips pub 46-2. **Federal Information Processing Standards Publication - National Institute of Standards and Technology**, [S.l.], Dezembro, 1993.

[NIS 93b] NIST. Secure hash standard - fips pub 180-1. **Federal Information Processing Standards Publication - National Institute of Standards and Technology**, [S.l.], Maio, 1993.

[NIS 00] NIST. Digital signature standard (dss) - fips pub 186-2. **Federal Information Processing Standards Publication - National Institute of Standards and Technology**, [S.l.], Janeiro, 2000.

[NIS 01a] NIST. Advanced encryption standard (aes) - fips pub 197. **Federal Information Processing Standards Publication - National Institute of Standards and Technology**, [S.l.], Novembro, 2001.

[NIS 01b] NIST. Security requirements for cryptographic modules - fips pub 140-2. **Federal Information Processing Standards Publication - National Institute of Standards and Technology**, [S.l.], Maio, 2001.

[OPE 02] OPENSSL. **OpenSSL**. Disponível em <http://www.openssl.org>. Acesso em 26 de Agosto de 2002.

[PAS 02] PASQUAL, E. S. **IDDE - Uma Infra-estrutura para a Datação de Documentos Eletrônicos**. Universidade Federal de Santa Catarina, 2002. Dissertação de Mestrado.

[PED 91] PEDERSEN, T. P. A threshold cryptosystem without a trusted party. **Advances in Cryptology - EUROCRYPT'91**, [S.l.], v.547, p.522–526, 1991.

[PHP 02] PHP. **PHP**. Disponível em <http://www.php.net>. Acesso em 26 de Agosto de 2002.

[RIV 78] RIVEST, R. L.; SHAMIR, A.; ADELMAN, L. M. A method for obtaining digital signatures and public-key cryptosystems. **Communications of the ACM**, [S.l.], v.21, n.2, Fevereiro, 1978.

[RIV 96] RIVEST, R. L.; SHAMIR, A.; WAGNER, D. A. Time-lock puzzles and timed-release crypto. <**http://theory.lcs.mit.edu/ rivest/RivestShamirWagner-timelock.pdf**>, [S.l.], , n.MIT/LCS/TR-684, Fevereiro, 1996.

[RIV 99] RIVEST, R. L. **Description of the LCS35 Time Capsule Crypto-Puzzle**. Disponível em <http://www.lcs.mit.edu/news/crypto.html>. Acesso em 06 de Setembro de 2002.

[ROO 99] ROOS, M. **Integrating Time-Stamping and Notarization**. University of Tartu - Estonia, Maio, 1999. Dissertação de Mestrado.

[SCH 96] SCHNEIER, B. **Applied Cryptography: Protocols, Algorithms, and Source Code in C**. 2. ed. John Wiley and Sons, Inc, 1996.

[SCH 99] SCHOENMAKERS, B. A simple publicly verificable secret sharing scheme and its application to electronic voting. **Advances in Cryptology - CRYPTO '99**, [S.l.], v.1666, p.148–164, 1999.

[SHA 79] SHAMIR, A. How to share a secret. **Communications of the ACM**, [S.l.], v.22, n.11, p.612–613, Novembro, 1979.

[SOA 91] SOARES, J. F.; DE FARIAS, A. A.; CESAR, C. C. **Introdução à Estatística**. Editora Guanabara Koogan S.A., 1991.

[STA 96] STADLER, M. Publicly verifiable secret sharing. **Advances in Cryptology - EUROCRYPT'96**, [S.l.], v.1070, p.190–199, 1996.

[STA 98] STALLINGS, W. **Cryptography and Network Security: Principles and Practice**. 2. ed. Prentice-Hall, Inc, 1998.

[STI 95] STINSON, D. R. **Cryptography: Theory and Practice**. CRC Press, 1995.

[STI 99] STINSON, D. R.; WEI, R. Unconditionally secure proactive secret sharing scheme with combinatorial structures. **Selected Areas in Cryptography**, [S.l.], p.200–214, 1999.

[STU 99] STUBBLEBINE, S. G.; SYVERSON, P. F. Fair on-line auctions without special trusted parties. **Lecture Notes in Computer Science**, [S.l.], v.1648, p.230–240, 1999.

[SUZ 02] SUZUKI, K.; YOKOO, M. Secure combinatorial auctions by dynamic programming with polynomial secret sharing. **Financial Cryptography 2002, Lecture Notes in Computer Science**, [S.l.], 2002.

[W3C 02] W3C. **HTML**. Disponível em <http://www.w3.org/MarkUp/>. Acesso em 16 de Agosto de 2002.

Apêndice A

Análise Probabilística

A.1 Introdução

Utilizando modelos probabilísticos torna-se possível inferir o quão seguro são os protocolos de criptografia temporal em grupos baseados em compartilhamento de segredos, através da atribuição de valores aos níveis de confiança oferecidos por cada membro do grupo participante de um protocolo.

Nestes protocolos a responsabilidade da segurança dos documentos eletrônicos é distribuída entre os membros do grupo através do esquema de compartilhamento de segredos de Shamir. Com isto, a segurança dos documentos somente é ameaçada em uma situação onde um mínimo de t membros deste grupo conspirem entre si e construam de maneira ilícita chaves *TKr* que possam vir a ser utilizadas na decifragem de documentos envolvidos no protocolo.

Este apêndice apresenta formas de analisar a segurança destes protocolos utilizando os modelos probabilísticos da *distribuição binomial* e da *distribuição de pascal*, os quais retratam por métodos diferentes as atitudes que podem ser tomadas por um agente malicioso que tenta persuadir a corrupção um certo número de membros do grupo.

A distribuição binomial retrata um cenário onde um agente malicioso, denominado aqui de corruptor, tenta persuadir a corrupção todo um subconjunto de mem-

bros de um grupo, visando o comprometimento da segurança do protocolo. Enquanto a distribuição de pascal retrata um cenário onde um corruptor tenta seqüencialmente persuadir a corrupção membros deste grupo, sendo que no momento em que ele obtém sucesso no comprometimento da segurança do protocolo, ele encerra as suas tentativas de persuasão.

A.2 Análise Utilizando Distribuição Binomial

Utilizando o modelo probabilístico da *distribuição binomial* [MEY 83, SOA 91], é possível determinar qual a probabilidade de comprometimento da segurança de um protocolo de criptografia temporal em grupos baseado em compartilhamento de segredos, se um corruptor tentar persuadir a corrupção um certo número de membros do grupo envolvido.

Esta distribuição considera um cenário onde todos os membros do protocolo em questão possuem probabilidades iguais e independentes de serem desonestos.

A análise de segurança de um protocolo utilizando esta distribuição consiste em determinar, através de expressões matemáticas, a probabilidade de **sucesso** que um corruptor tem, se ele tentar persuadir um número k ($t \leq k \leq n$) de membros, considerando que estes membros possuem probabilidades *p* de serem desonestos. Considera-se como **sucesso** do corruptor, o fato dele conseguir corromper um número de membros **igual ou maior** do que o necessário para comprometer a segurança do protocolo (equivalente ao valor de t).

O resultado obtido com a análise permite mensurar os níveis de segurança (*seg*) e de comprometimento (*comp*) oferecidos pelo protocolo. Abaixo segue a notação utilizada na análise:

- n: número total de membros atuantes no protocolo;
- t: número de membros necessários para comprometer a segurança do protocolo ($t \leq n$);
- k: número de fornecedores induzidos pelo corruptor a corrupção ($t \leq k \leq n$);

- *p*: probabilidade de um membro ser desonesto;
- *comp*: probabilidade de comprometimento da segurança do protocolo;
- *seg*: probabilidade de não comprometimento da segurança do protocolo;
- $\mathcal{C}_t^k$: Combinação de k, t a t, cujo resultado é dado pela expressão: $\mathcal{C}_t^k = \frac{k!}{t!(k-t)!}$

A probabilidade de sucesso que um corruptor terá se ele tentar corromper um número de k membros do grupo é dada pela expressão:

$$comp = \sum_{s=t}^{k} \mathcal{C}_s^k \;\; p^s(1-p)^{k-s}$$

Enquanto o nível de segurança oferecido pelo protocolo, o qual representa a probabilidade da segurança do protocolo não ser comprometida, é dada pela expressão:

$$seg = 1 - comp$$

Visando uma melhor compreensão, é apresentado abaixo um exemplo numérico onde são analisadas as probabilidades de **comprometimento** e **não comprometimento** apresentados por um protocolo de criptografia temporal baseado em compartilhamento de segredos.

Exemplo: Seja um protocolo com os seguintes parâmetros: n = 10, t = 6 e p = 0,50. A análise é realizada considerando 3 cenários distintos os quais atribuem diferentes valores ao parâmetro k.

Cenário 1: O corruptor tenta persuadir a corrupção 6 membros do grupo (k = 6):

$$comp = \frac{6!}{6!(6-6)!} \times 0,50^6 \times 0,50^0 \quad \Longrightarrow \quad 0,0156\ (1,56\%)$$

$$seg = 1 - 0,0156 \quad \Longrightarrow \quad 0,9844\ (98,44\%)$$

Cenário 2: O corruptor tenta persuadir a corrupção 8 membros do grupo (k = 8):

$$comp_1 = \frac{8!}{6!(8-6)!} \times 0,50^6 \times 0,50^2 \implies comp_1 = 0,1093$$
$$comp_2 = \frac{8!}{7!(8-7)!} \times 0,50^7 \times 0,50^1 \implies comp_2 = 0,0312$$
$$comp_3 = \frac{8!}{8!(8-8)!} \times 0,50^8 \times 0,50^0 \implies comp_3 = 0,0039$$

portanto

$$comp = 0,1093 + 0,0312 + 0,0039 \implies 0,1444\ (14,44\%)$$

$$seg = 1 - 0,1444 \implies 0,8556\ (85,56\%)$$

Cenário 3: O corruptor tenta persuadir a corrupção 10 membros do grupo (k = 10):

$$comp_{f_1} = \frac{10!}{6!(10-6)!} \times 0,50^6 \times 0,50^4 \implies comp_1 = 0,2050$$
$$comp_{f_2} = \frac{10!}{7!(10-7)!} \times 0,50^7 \times 0,50^3 \implies comp_2 = 0,1171$$
$$comp_{f_3} = \frac{10!}{8!(10-8)!} \times 0,50^8 \times 0,50^2 \implies comp_3 = 0,0439$$
$$comp_{f_4} = \frac{10!}{9!(10-9)!} \times 0,50^9 \times 0,50^1 \implies comp_4 = 0,0097$$
$$comp_{f_5} = \frac{10!}{10!(10-10)!} \times 0,50^{10} \times 0,50^0 \implies comp_5 = 0,0009$$

portanto

$$comp = 0,2050 + 0,1171 + 0,0439 + 0,0097 + 0,0009 \implies 0,3766\ (37,66\%)$$

$$seg = 1 - 0,03766 \implies 0,6234\ (62,34\%)$$

Os resultados obtidos nos exemplos permitem a visualização do aumento gradativo das chances de sucesso do corruptor a medida em que o número de entidades que ele tenta persuadir aumenta. A tabela A.1 compara estes resultados.

Tabela A.1: Comparativo dos resultados obtidos nos exemplos de análise de segurança utilizando distribuição binomial.

Cenário	Probabilidade de comprometimento	Probabilidade de não comprometimento
1	$1,56\%$	$98,44\%$
2	$14,44\%$	$85,56\%$
3	$37,66\%$	$62,34\%$

A.3 Análise Utilizando Distribuição de Pascal

A distribuição de pascal, também conhecida como *distribuição binomial negativa* [MEY 83, SOA 91], traduz a probabilidade de k ($t \leq k \leq n$) ser o número de membros que o corruptor deve tentar persuadir até conseguir obter **sucesso** no comprometimento da segurança do protocolo, sendo que o sucesso somente ocorre quando o *k-ésimo* membro for corrompido. Nesta análise considera-se como **sucesso** o fato do corruptor conseguir corromper **exatamente** o número de membros necessários ao comprometimento da segurança do protocolo (equivalente ao valor de t).

Nesta distribuição também considera-se um cenário onde todos os membros do protocolo em questão possuem probabilidades iguais e independentes de serem desonestos.

A notação utilizada nesta análise é descrita abaixo:

- n: número total de membros atuantes no protocolo;
- t: número de membros necessários para comprometer a segurança do protocolo ($t \leq n$);
- k: número de tentativas até que o *t-ésimo* membro seja corrompido;
- *p*: probabilidade de um membro ser desonesto;
- $comp$: probabilidade de que o *t-ésimo* membro corrupto seja alcançado quando o *k-ésimo* membro for considerado;
- seg: probabilidade de que o *t-ésimo* membro corrupto não seja alcançado quando o *k-ésimo* membro for considerado;
- $\mathcal{C}_t^k$: Combinação de k, t a t, cujo resultado é dado pela expressão: $\mathcal{C}_t^k = \frac{k!}{t!(k-t)!}$

Portanto, a probabilidade de que o *t-ésimo* membro corrompido ocorra na *k-ésima* tentativa é dada pela expressão:

$$comp = \mathcal{C}_{t-1}^{k-1} p^t (1-p)^{k-t}$$

Já a probabilidade do corruptor não obter sucesso no comprometimento da segurança do protocolo quando considerado o *k-ésimo* membro é dada pela expressão:

$$seg = 1 - comp$$

Abaixo é apresentado um exemplo onde são analisadas as probabilidades de **comprometimento** e **não comprometimento** apresentados por um protocolo de criptografia temporal baseado em compartilhamento de segredos.

Exemplo: Seja um protocolo com os seguintes parâmetros: n = 10, t = 6 e p = 0,50. A análise é realizada considerando 3 cenários distintos, os quais atribuem diferentes valores ao parâmetro k.

Cenário 1: O corruptor tenta persuadir a corrupção 6 membros do grupo até que o *t-ésimo* seja corrompido, k = 6:

$$prob = \frac{5!}{5!(5-5)!} \times 0,50^6 \times 0,50^0 \quad \Longrightarrow \quad 0,0156\ (1,56\%)$$

$$seg = 1 - 0,156 \quad \Longrightarrow \quad 0,9844\ (98,44\%)$$

Cenário 2: O corruptor tenta persuadir a corrupção 8 membros do grupo até que o *t-ésimo* seja corrompido, k = 8

$$prob = \frac{7!}{5!(7-5)!} \times 0,50^6 \times 0,50^2 \quad \Longrightarrow \quad 0,0820\ (8,20\%)$$

$$seg = 1 - 0,0820 \quad \Longrightarrow \quad 0,9180\ (91,80\%)$$

Cenário 3: O corruptor tenta persuadir a corrupção 10 membros do grupo até que o *t-ésimo* seja corrompido, k = 10:

$$prob = \frac{9!}{5!(9-5)!} \times 0,50^6 \times 0,50^4 \quad \Longrightarrow \quad 0,1230\ (12,30\%)$$

$$seg = 1 - 0,1230 \quad \Longrightarrow \quad 0,8770\ (87,70\%)$$

Novamente é possível visualizar, através dos resultados obtidos, que à medida em que o corruptor tenta induzir mais membros, ele se aproxima do número ideal de membros que lhe permite comprometer a segurança do protocolo. A tabela A.2 compara estes resultados.

Tabela A.2: Tabela comparativa dos resultados obtidos nos exemplos de análise de segurança utilizando distribuição de pascal.

Cenário	Probabilidade de comprometimento	Probabilidade de não comprometimento
1	$1,56\%$	$98,44\%$
2	$8,20\%$	$91,80\%$
3	$12,30\%$	$87,70\%$

A.4 Probabilidades diferentes entre membros

Os modelos probabilísticos utilizados até o momento consideram somente a igualdade e independência de probabilidades de desonestidade entre os membros de um grupo. No entanto, esta situação não ocorre na prática, pois usualmente pessoas possuem princípios diferentes e por conseqüência probabilidades maiores ou menores de serem desonestas.

Porém, nos estudos realizados não foram encontrados modelos probabilísticos capazes de retratar este cenário.

Apêndice B

Sistema Seguro de Compras

B.1 Introdução

O sistema desenvolvido neste trabalho representa o protótipo inicial do **sistema seguro de compras**, objeto do projeto **Processo CompraS** em desenvolvimento no **LabSEC**. Este projeto visa a construção de um sistema que assegure, através de recursos da Tecnologia de Segurança da Informação, a realização via Internet de todas as etapas que compreendem um processo de compra, em particular processos de licitação pública.

O desenvolvimento do sistema contou com a colaboração de dois alunos[1] da graduação do curso de Ciência da Computação da UFSC.

A seção B.2 apresenta o sistema desenvolvido e a seção B.3 cita as tecnologias utilizadas no desenvolvimento e apresenta de forma geral as principais funcionalidades do sistema.

B.2 Apresentação

O sistema desenvolvido consiste em um ambiente WEB destinado à realização de processos de licitação pública voltados para compras. O protocolo de crip-

[1] Iuri Campana e Victor Simas Silva

tografia temporal implementado é utilizado para prover a garantia da confidencialidade das propostas de preço, entregues ao comprador, durante o período de tempo que representa a fase de envio de propostas. Após expirado este período o protocolo assegura a abertura de todas as propostas entregues. O protocolo implementado foi o protocolo 2, baseado em compartilhamento de segredos, descrito na seção 6.4.3.

No sistema desenvolvido foi necessária a implementação de alguns passos que compreendem o protocolo de envio de propostas em processos de compras, proposto no capítulo 7. Estes passos são necessários à execução do protocolo de criptografia temporal para grupos em um processo de licitação.

O sistema compõe um ambiente onde são oferecidos os procedimentos de:

1. Elaboração e publicação do edital;
2. Formação do grupo que atuará no protocolo;
3. Execução do protocolo de criptografia temporal para grupos;
4. Envio de propostas cifradas e assinadas pelos fornecedores;
5. Abertura e análise do conteúdos dos envelopes entregues;
6. Publicação da proposta vencedora.

A elaboração e publicação de editais são serviços disponbilizados a usuários cadastrados na categoria **compradores**. Estes usuários podem preencher o resumo de um edital através do sistema e anexar a este um documento que represente o edital em sua íntegra. Após estes passos o usuário disponibiliza este edital na área pública do sistema.

A formação do grupo é realizada através da etapa de comprometimento descrita no protocolo de envio de propostas, na qual o fornecedor interessado envia um termo onde declara a concordância com as condições estabelecidas no edital e seu interesse em participar do processo de licitação. Junto a este termo, o fornecedor deve

informar a chave F_i*TKu* que utilizará na cifragem da sua proposta. Esta chave é utilizada pelos demais fornecedores no momento do compartilhamento das chaves *TKr*.

As chaves F_i*TKr* e F_i*TKu* devem estar contidas em um certificado digital instalado na máquina de F_i.

A execução do protocolo de criptografia temporal é realizada de maneira automática e transparente a F_i, juntamente com o envio da sua proposta cifrada e assinada.

A execução do protocolo de criptografia temporal exige computação no lado cliente da aplicação, nas máquinas de usuários **compradores** e **fornecedores**. É importante ressaltar, que todos os serviços de criptografia necessários são realizados no lado cliente da aplicação. Somente é realizado no lado servidor a criação de um canal de comunicação privado entre cliente e servidor.

A decifragem e análise das propostas entregues é realizado pelo comprador, que após a escolha tem a opção de divulgar a proposta vencedora através da área pública do sistema.

B.3 Implementação

O sistema é constituído de aplicações que são executadas no lado cliente e servidor da aplicação. O lado cliente da aplicação foi desenvolvido visando operar sobre o sistema operacional Windows 2000 [MIC 02f], através do navegador Internet Explorer [MIC 02d]. O lado servidor foi desenvolvido visando operar sobre o sistema operacional Linux Red Hat [HAT 02], através do servidor WEB Apache [APA 02].

A escolha das tecnologias utilizadas no lado servidor foi motivada pela robustez que elas apresentam e pela sua consagração como a combinação *servidor WEB / sistema operacional* mais utilizada atualmente. Outro requisito considerado foi o suporte à ferramenta OpenSSL [OPE 02] oferecido pelo Linux, utilizada no suporte ao canal de comunicação privado SSL [STA 98] criado entre servidor e cliente.

A independência de plataformas no lado cliente não foi objetivo no desenvolvimento do sistema, uma vez que o seu uso comercial não é imediato.

As plataformas de programação utilizadas no desenvolvimento do sistema constituem-se em: linguagens de programação PHP[PHP 02], JavaScript [MIC 02c], VBScript [MIC 02e] e HTML [W3C 02], banco de dados MySQL [MYS 02], ferramenta OpenSSL [OPE 02] e biblioteca de suporte a criptografia CAPICOM [MIC 02a].

B.3.1 Lado Servidor

A atribuição principal do servidor da aplicação é a de intermediar a comunicação entre comprador e fornecedores. Os dados mantidos pelo servidor são, em sua maioria, cifrados com as chaves públicas dos respectivos destinatários, impedindo com isso o eventual comprometimento da confidencialidade destes dados através de um ataque ao servidor.

As demais atribuições do servidor são:

- Autenticar usuários através de certificados digitais;
- Criar um canal de comunicação privado SSL entre servidor e cliente;
- Manter disponíveis as páginas e o componente que compõem o sistema;
- Gerenciar o banco de dados.

O componente citado terá sua funcionalidade descrita na seção subseqüente.

B.3.2 Lado Cliente

Os principais procedimentos realizados no lado cliente referem-se a execução dos serviços de criptografia necessários. Estes serviços constituem-se na cifragem, decifragem e assinatura de dados bem como a execução dos protocolos de construção e reconstrução do esquema de Shamir (seção 3.4.1).

Os passos que compreendem o protocolo de criptografia temporal adotado foram implementados em um componente desenvolvido na linguagem de programa-

ção VBScript, fazendo uso de serviços de criptografia oferecidos pela biblioteca CAPICOM.

No início dos procedimentos de envio da proposta, este componente é carregado na máquina do fornecedor, realizando em seguida a cifragem e assinatura da proposta. No passo seguinte o componente solicita ao fornecedor uma senha e a utiliza na exportação do certificado digital que contém a chave F_i*TKr*. A exportação do certificado digital contendo esta chave foi necessária devido a restrições impostas pela CAPICOM quanto a manipulação de chaves criptográficas não contidas em certificados digitais.

A senha utilizada na exportação do certificado contendo a chave *TKr* é quebrada através do esquema de Shamir. As partes geradas são cifradas com as chaves *TKu* dos respectivos destinatários, informadas pelos fornecedores no momento da formação do grupo.

Após encerrado a fase de envio de propostas, o comprador solicita a todos os demais membros do grupo o envio espontâneo das senhas que eles utilizaram na exportação dos certificados digitais que contém suas chaves *TKr*. O não envio da senha por algum fornecedor torna necessária a reconstrução desta. A reconstrução somente é possível caso o comprador tenha recebido no mínimo t chaves *TKr* dos demais fornecedores. Desta maneira o comprador as utiliza para decifrar as partes, mantidas no servidor, da senha do fornecedor que negou o envio.

Os procedimentos de decifragem das propostas e reconstrução de senhas também são realizados pelo componente.

A ação do componente é definida de acordo com o momento do processo de licitação e a categoria em que o usuário é enquadrada.